Internetworking With Cisco Switches

Objectives

- Understand OSI model as it pertains to switches.
- Recognize various switch indicators.
- List the advantages of switches.
- Understand switch functions and operation.
- Understand the various switch protocols including VTP, HSRP and STP.

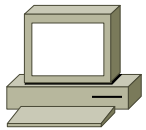
Objectives (cont.)

- Understand Cisco's Network Hierarchy model.
- Demonstrate knowledge of VLAN advantages, configuration and advanced options.
- Understand trunking, encapsulation and etherchannels.
- Configure switches using 5 step model.

Graphic Symbols

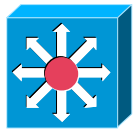
Bridge

Switch



Personal computer

Network switch

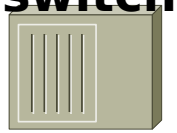


Multi-layer switch

Router

Web Server

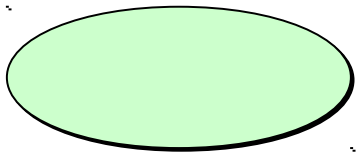
File Server



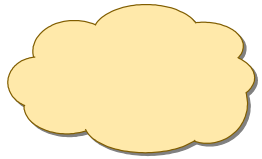
Hub

Modem

WAN “cloud”

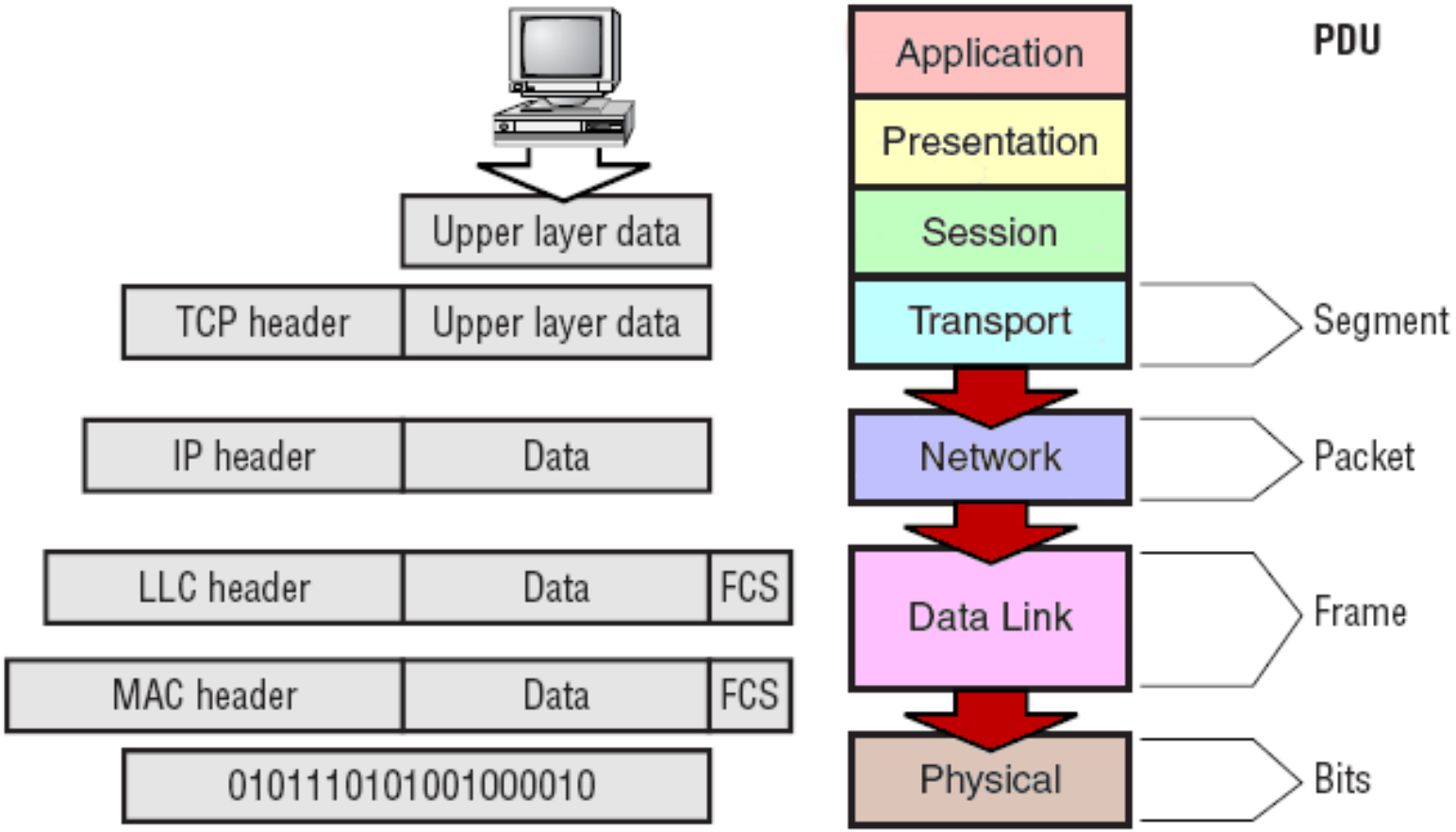


VLAN

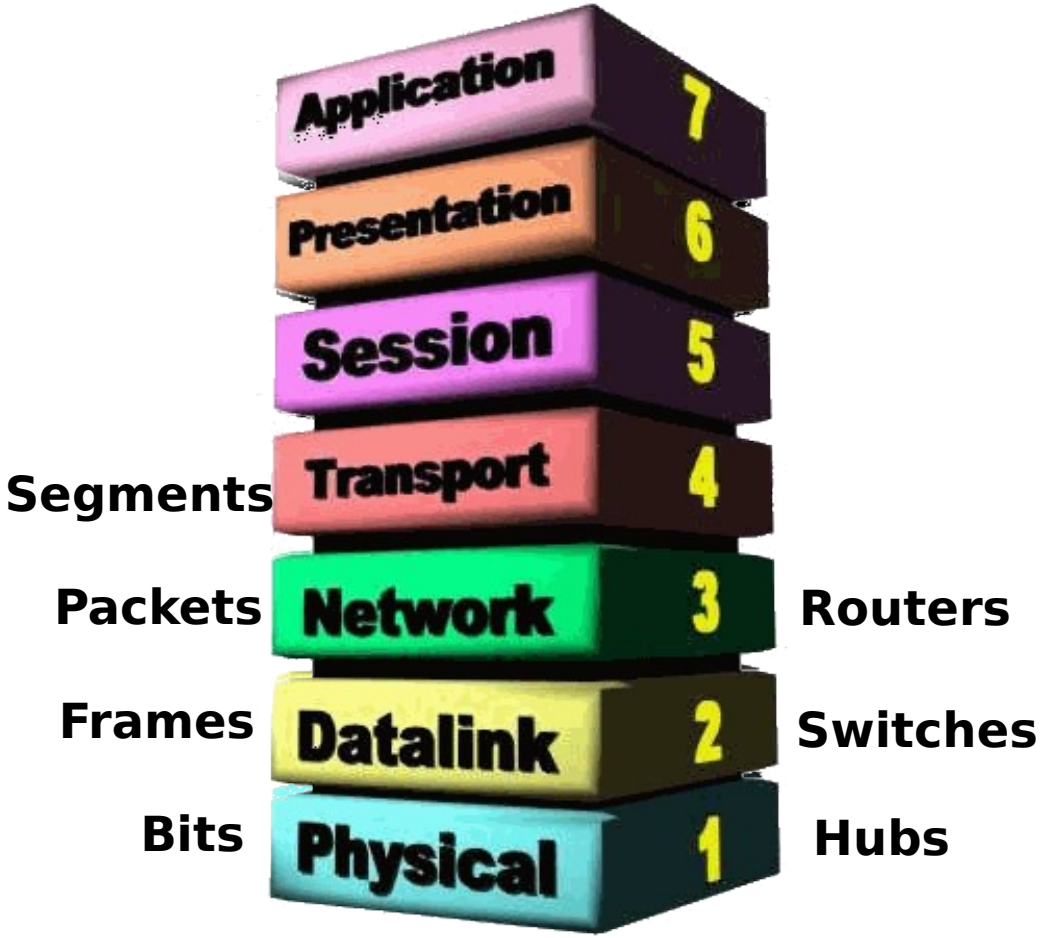


Network Cloud or Broadcast Domain

OSI Model Overview



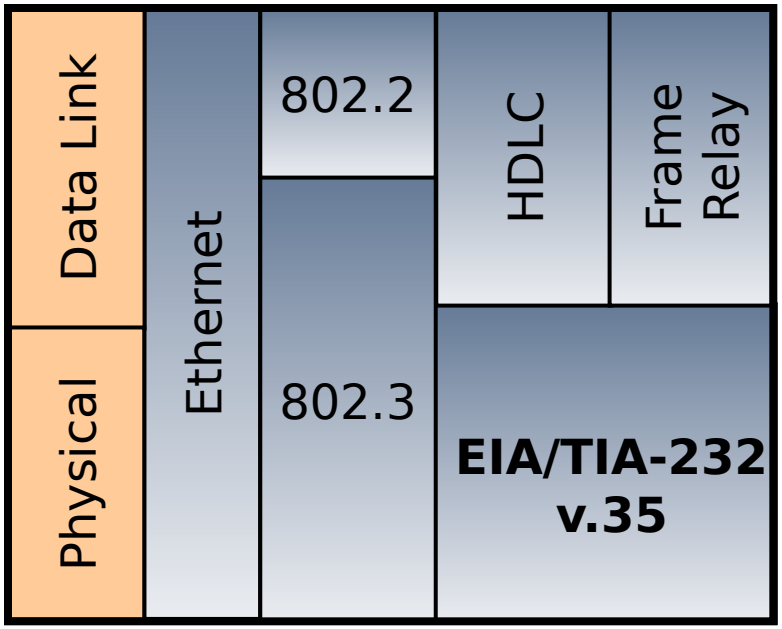
OSI Model Overview (cont.)



OSI Model Overview (cont.)

Segment

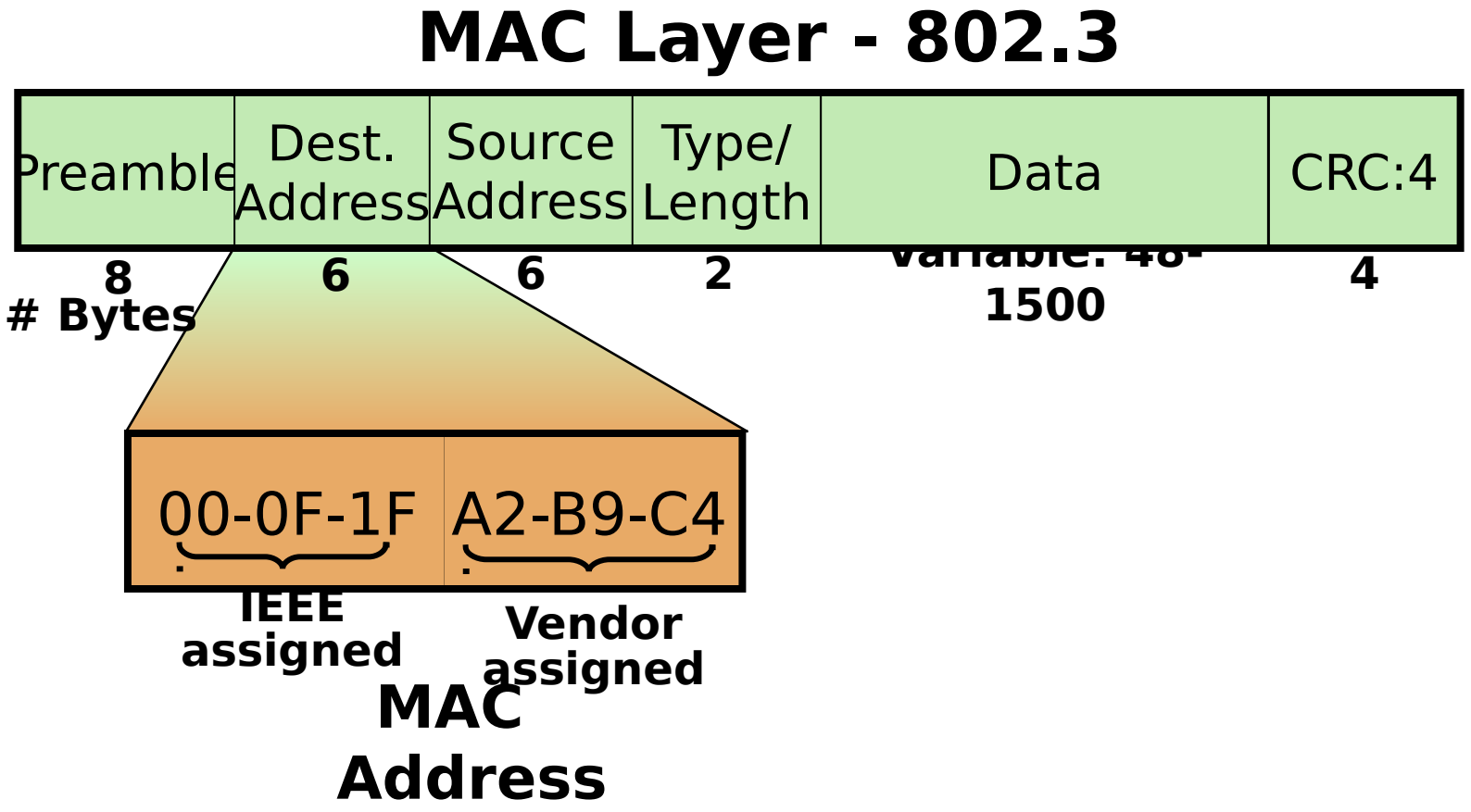
Physical & Data Link



Define

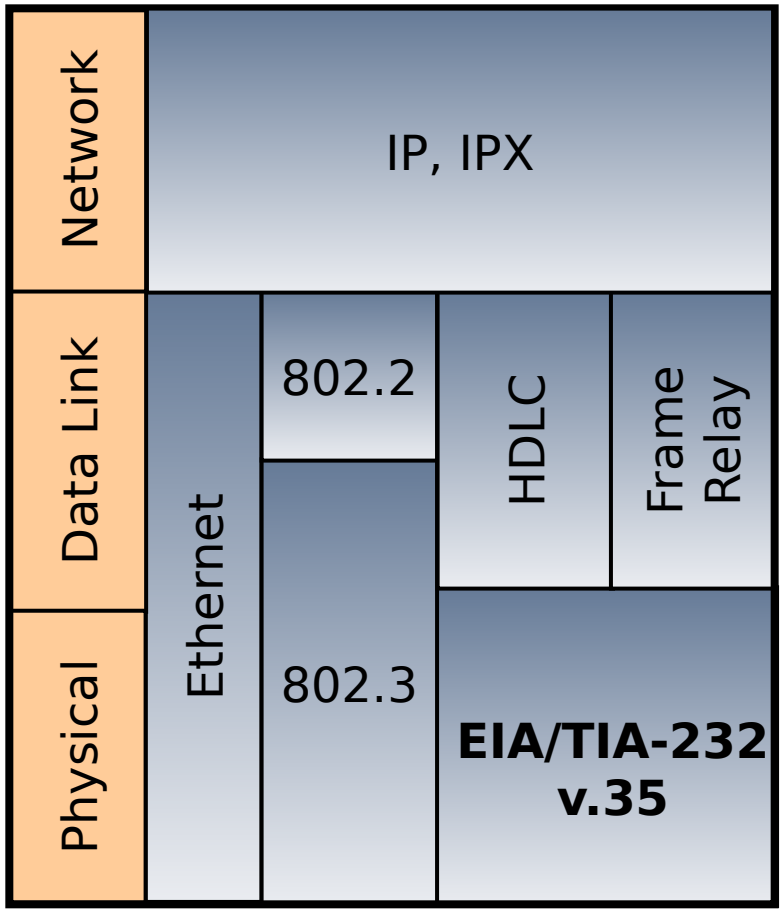
- Physical source and destination addresses
- Higher layer protocol (Service Access Point) associated with frames
- Network topology
- Frame sequencing
- Flow control
- Connection-oriented or connectionless

Data Link Layer



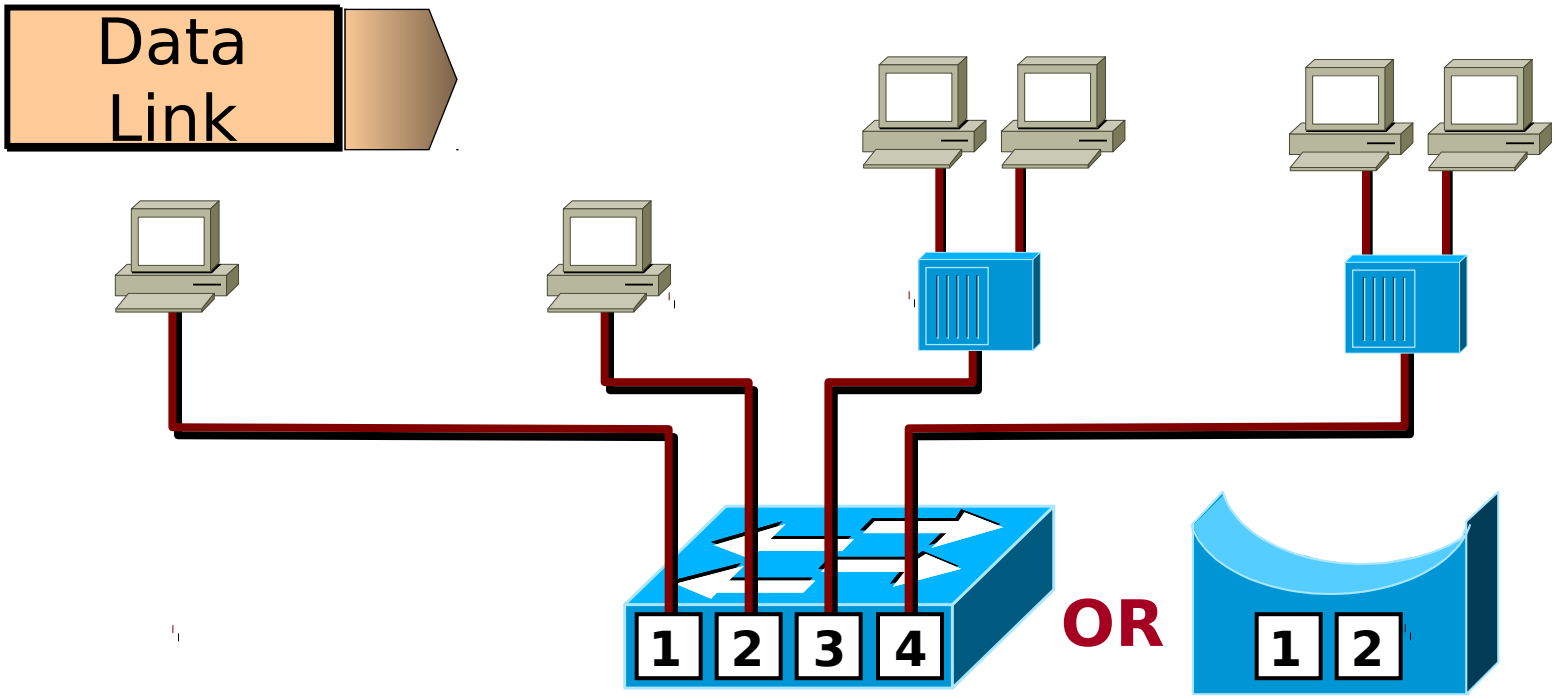
Network Layer Functions

MSTP



- Defines logical source and destination addresses associated with a specific protocol
- Defines paths through network
- Interconnects multiple data links

Switches, Bridges, Hubs



- **Each segment has own collision domain**
- **All segments are in same broadcast domain**

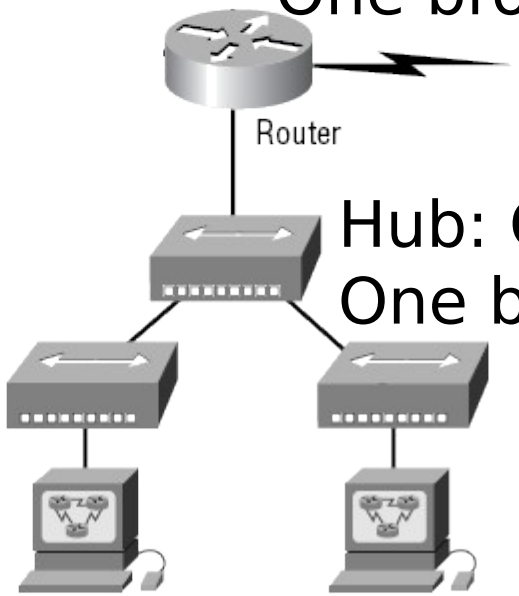
Function of a Switch

- Layer 2 Switching is Hardware Based
  - Application-Specific Integrated Circuits (ASICs)
  - No modification to Layer 2 Header
- Break Up Collision Domains
- Provide Segmentation
  - Each Port is a segment
- Can achieve Gigabit Speeds

Function of a Switch (cont.)

Switch: Many collision domains
One broadcast domain

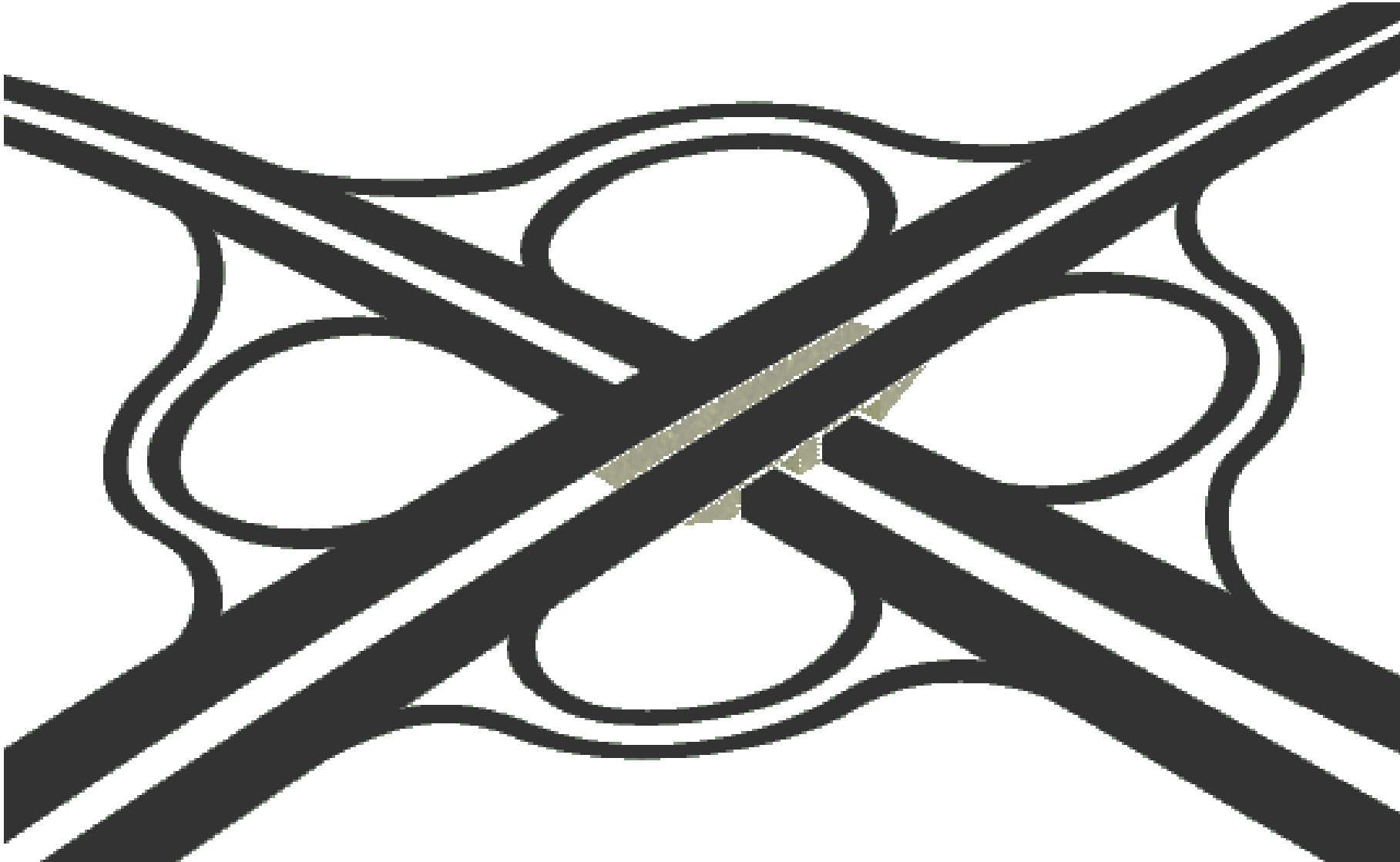
Bridge: 3 collision domain
One broadcast domain



Hub: One collision doma
One broadcast domain

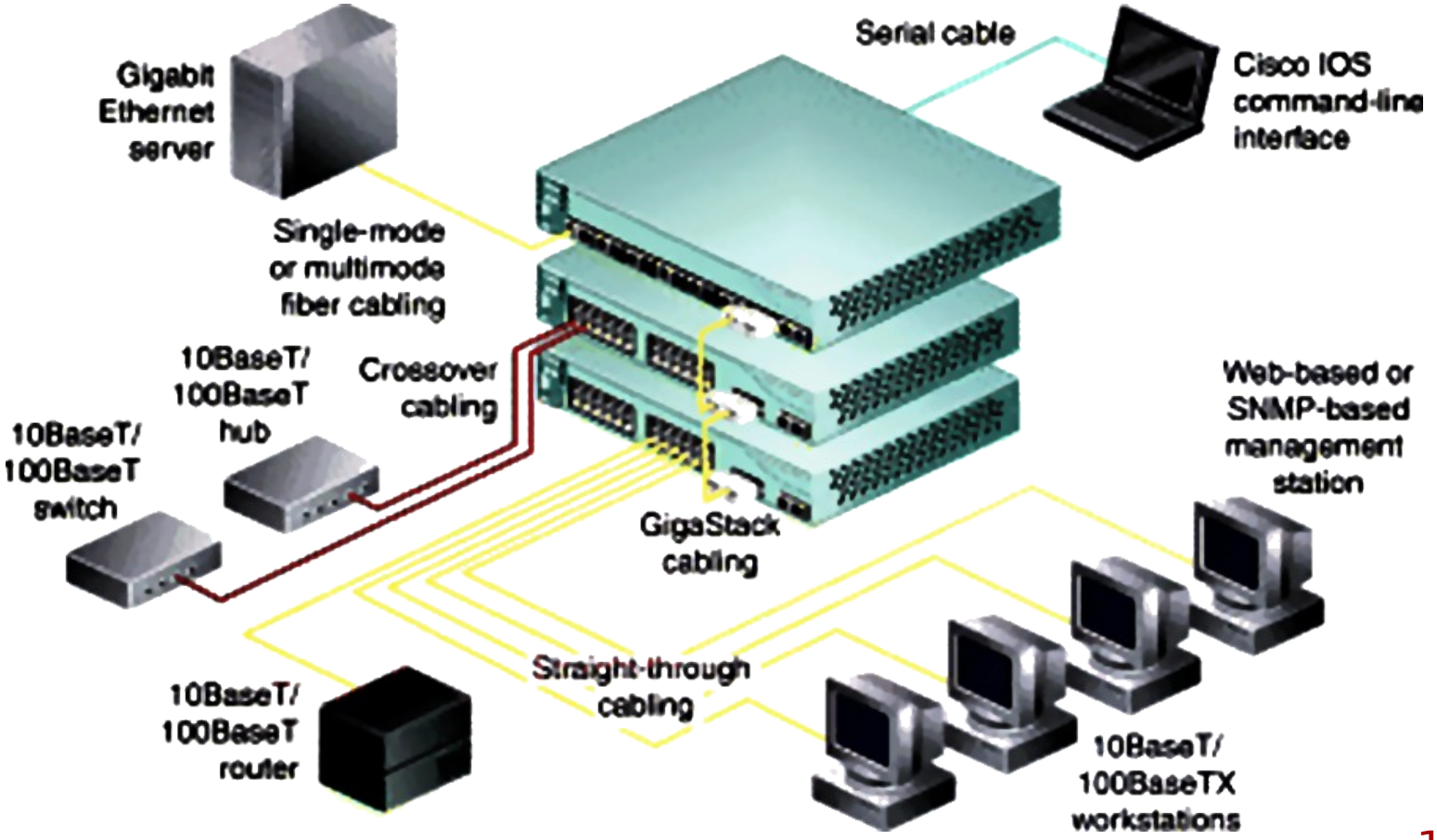
Hubs

Switches



Typical Switched Network

MSTP



Switch Advantages

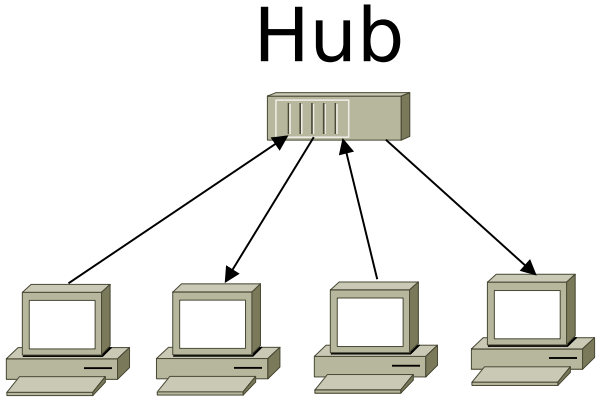
- Each segment has its own collision domain
- Broadcasts are forwarded to all segments
- Switching allows a network to maintain full-duplex Ethernet.

Data Flow

MSTP

Half duplex (CSMA/CD)

- Unidirectional data flow
- Higher potential for collisions
- Hubs connectivity

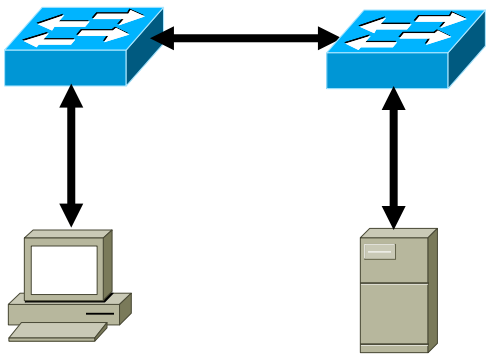


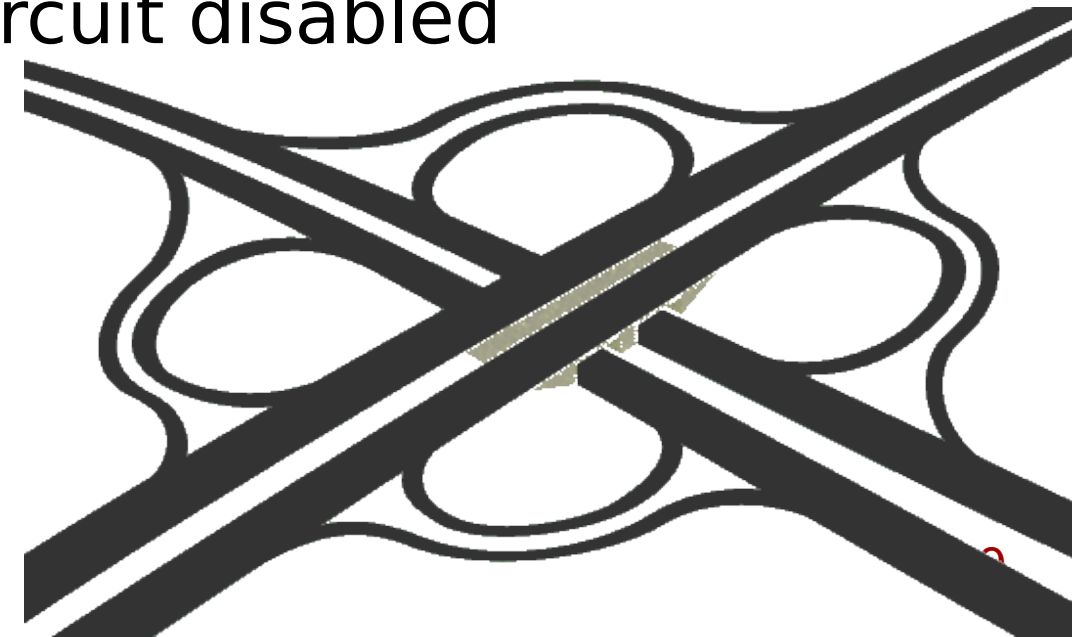
Data Flow (cont.)

Full duplex

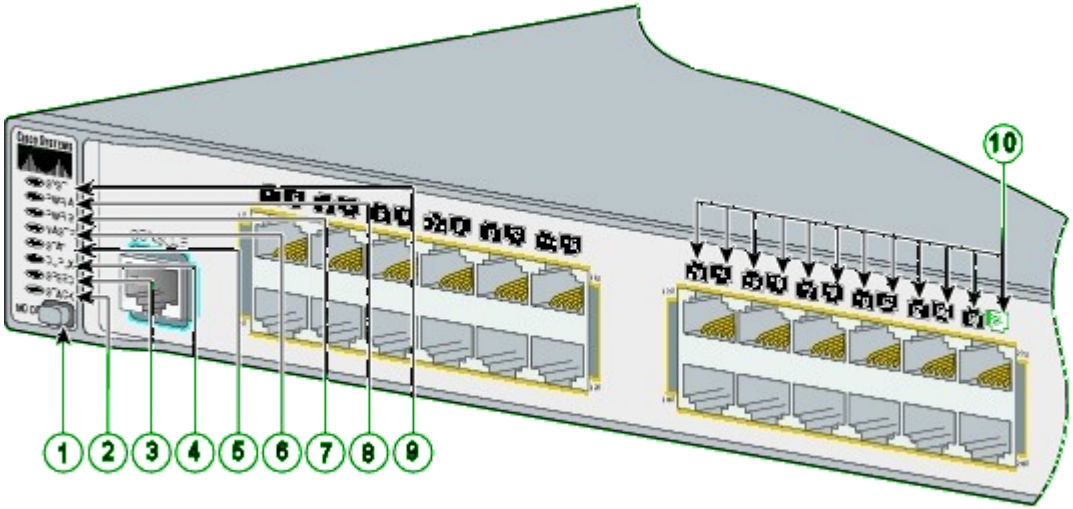
- Point-to-point only
- Attached to dedicated switched port
- Requires full-duplex support on both ends
- Collision free
- Collision detect circuit disabled

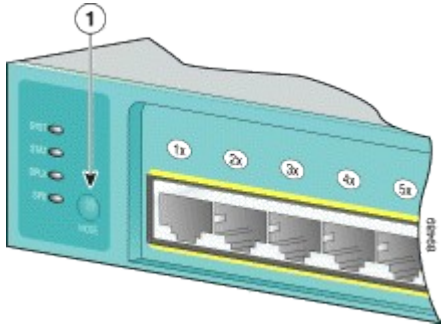
Switches





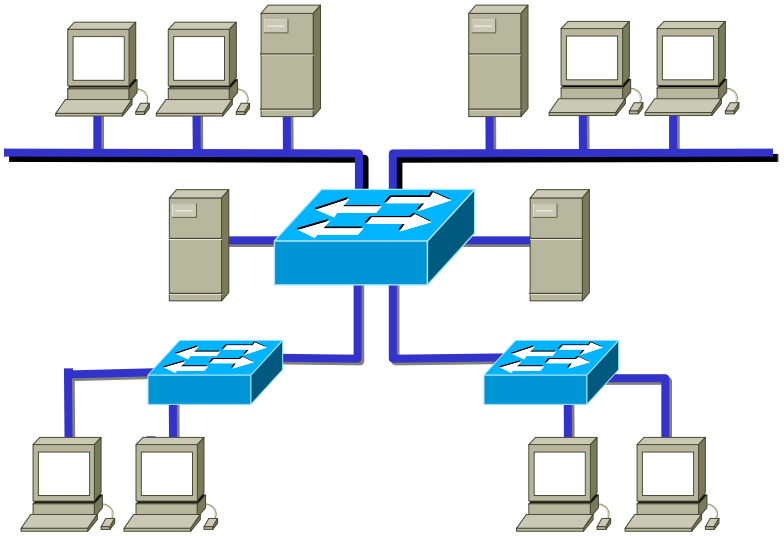
Switch Fronts





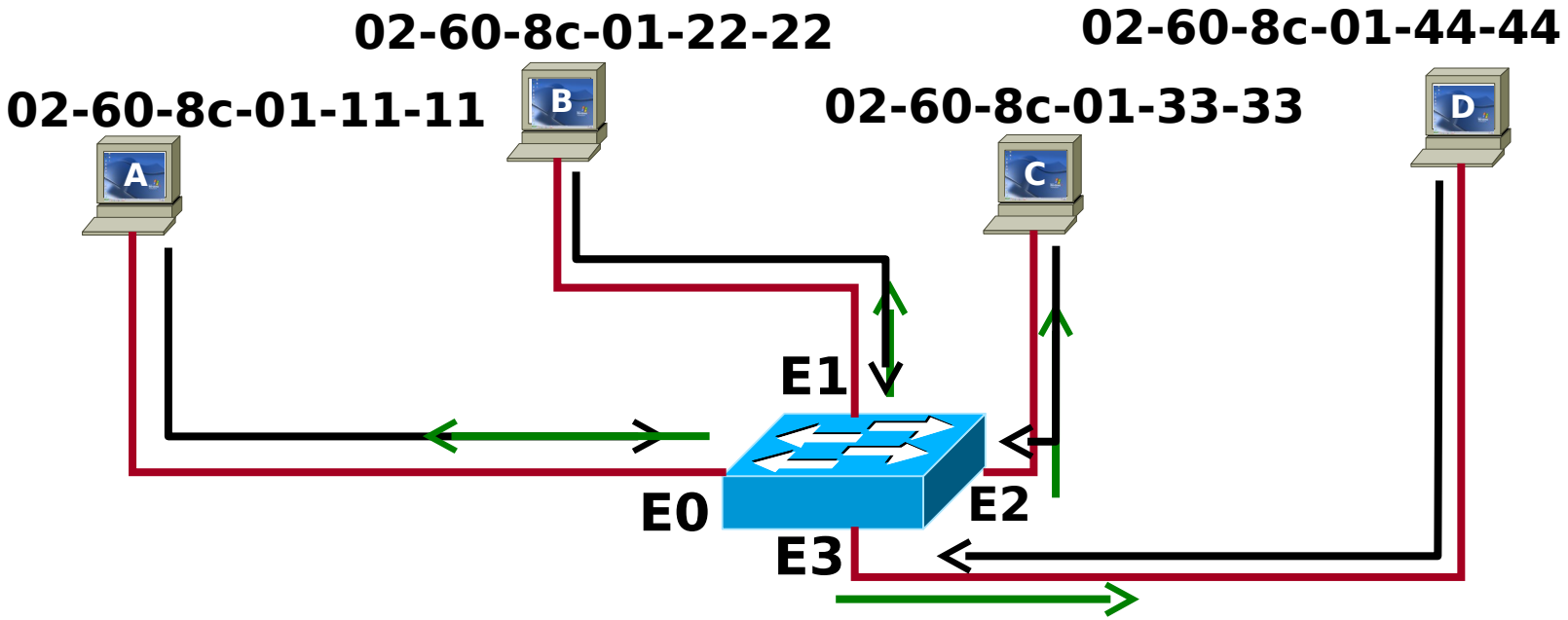
1	Mode button	6	Master LED
2	Stack LED (not used in this release)	7	Power B LED
3	Speed LED	8	Power A LED
4	Duplex LED	9	System LED
5	Status LED	10	Port LED

How it Works



- Address learning
- Forward/filter decision
- Loop avoidance

Address Learning



MAC address table

E0 = 02-60-8c-01-11-11
E3 = 02-60-8c-01-44-44
E2 = 02-60-8c-01-33-33
E1 = 02-60-8c-01-22-22

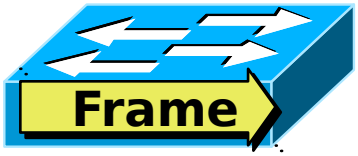
LAN Switching

There are three different methods used to filter or forward frames:

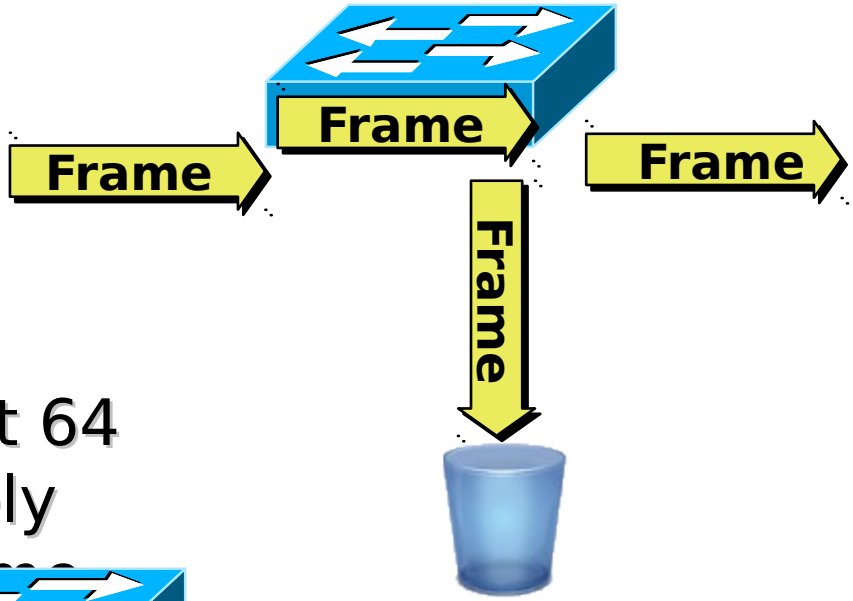
- **Cut-Through**
- **Store-and-Forward**
- **Fragment Free**

LAN Switching (cont.)

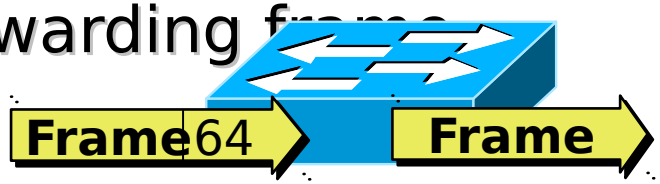
- Cut-through
  - Switch checks destination address and immediately begins forwarding frame



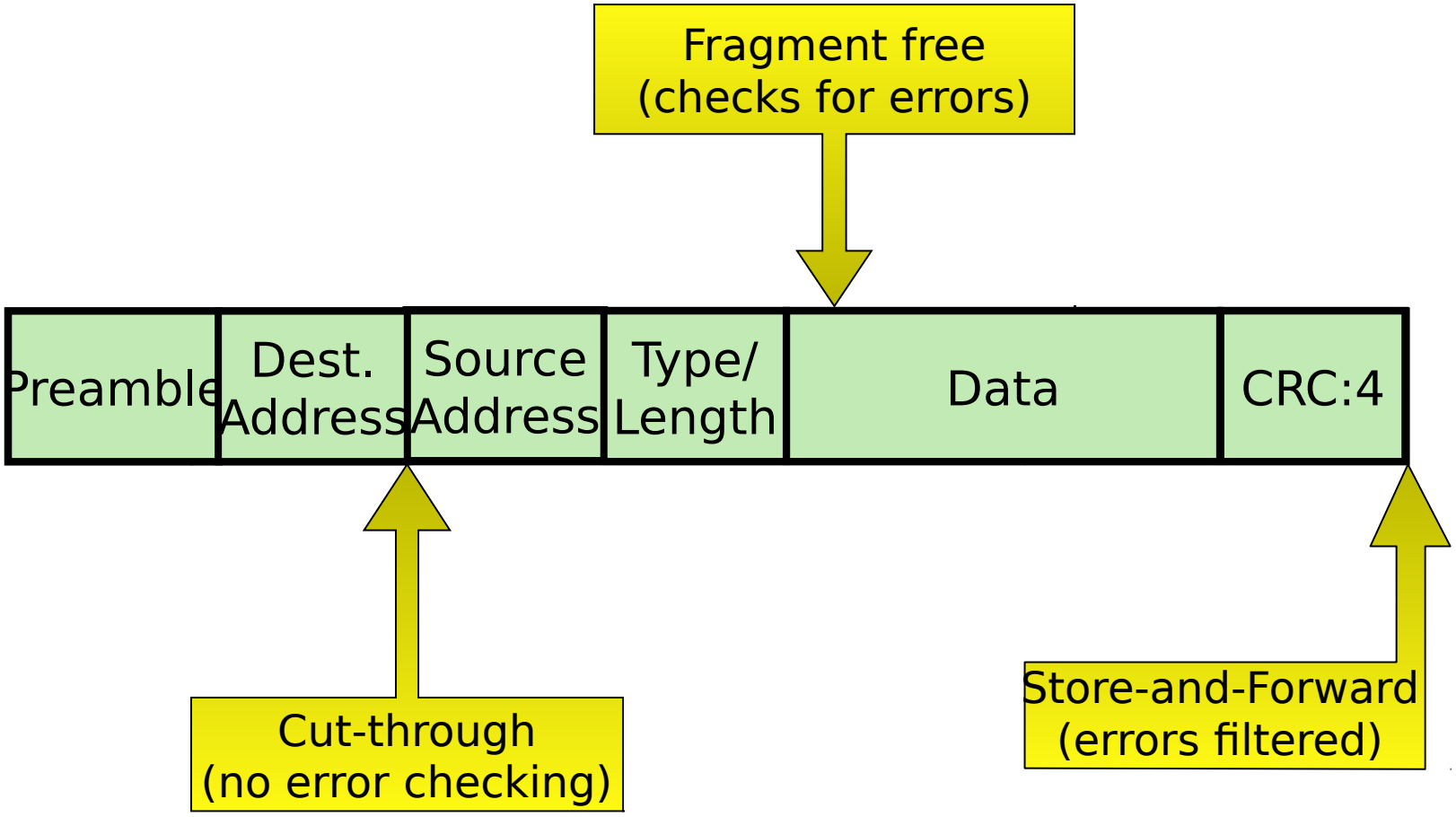
- Store and forward
  - Complete frame is received and checked before forwarding



- Fragment free (modified cut-through)
  - Switch checks the first 64 bytes then immediately begins forwarding frame



LAN Switching (cont.)

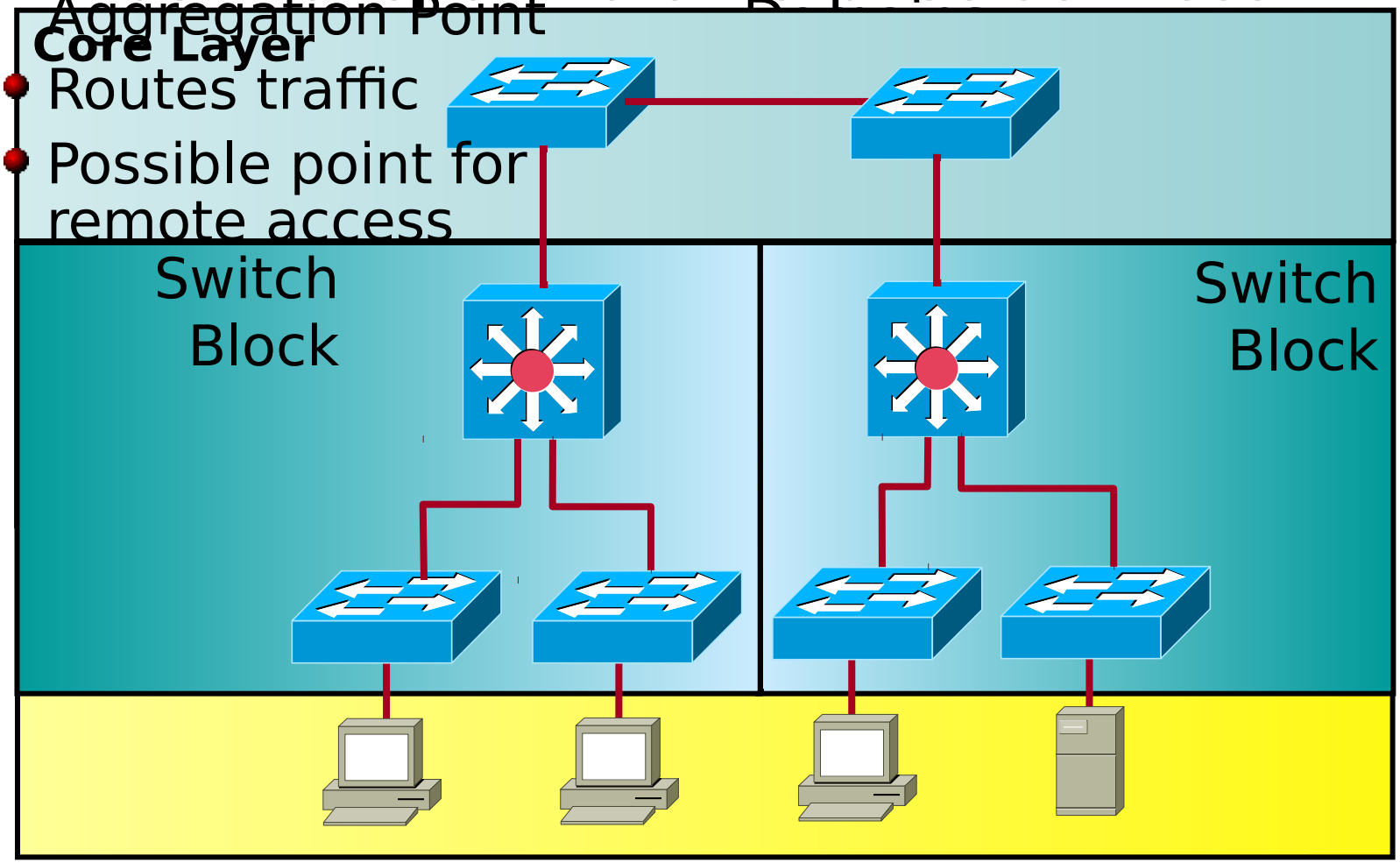


Cisco's Network Hierarchy

- Access Layer
  - Aggregation Point
- Broadcast/Multicast
  - Fast transport to enterprise services

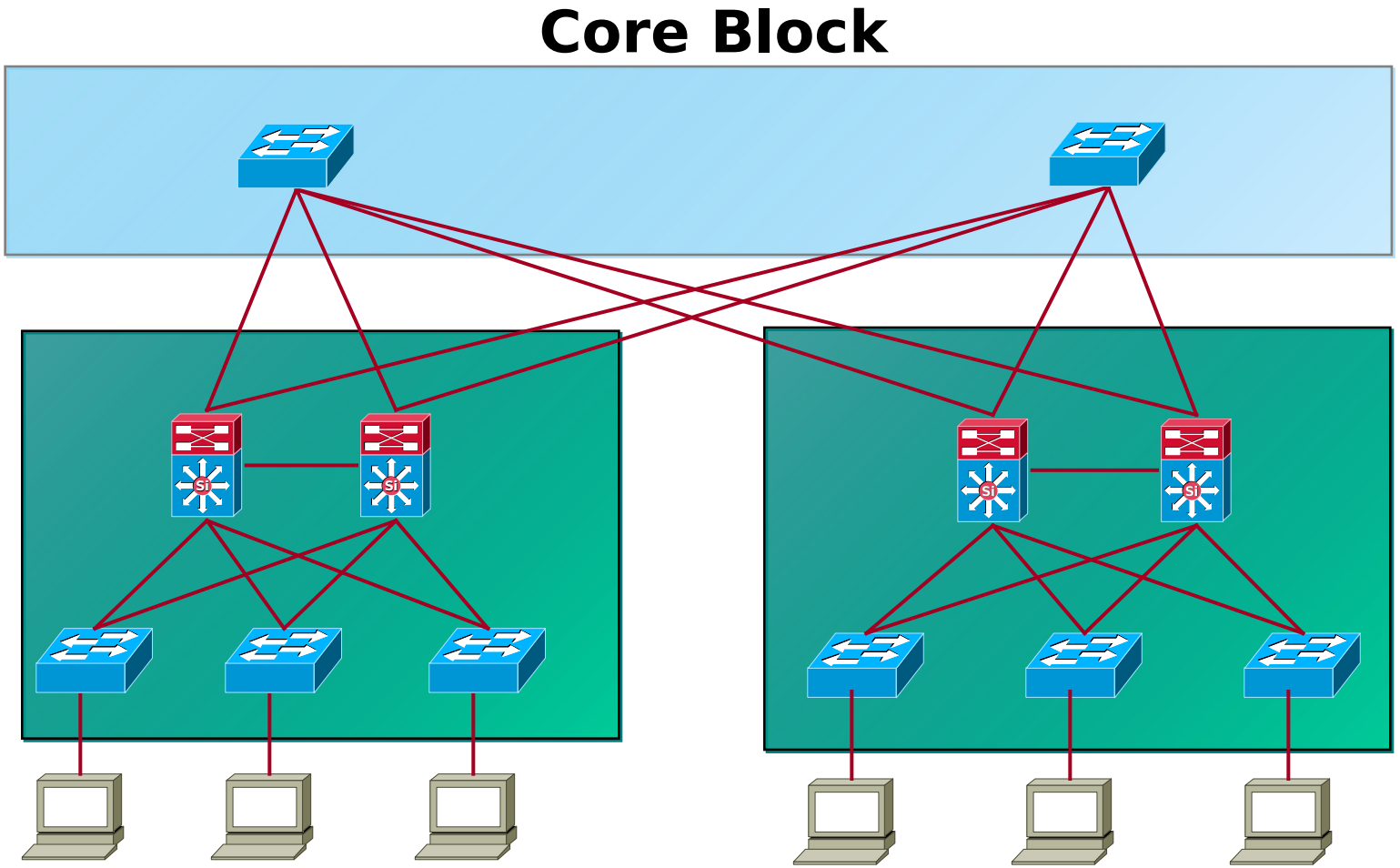
Core Layer

- Routes traffic
- Possible point for remote access



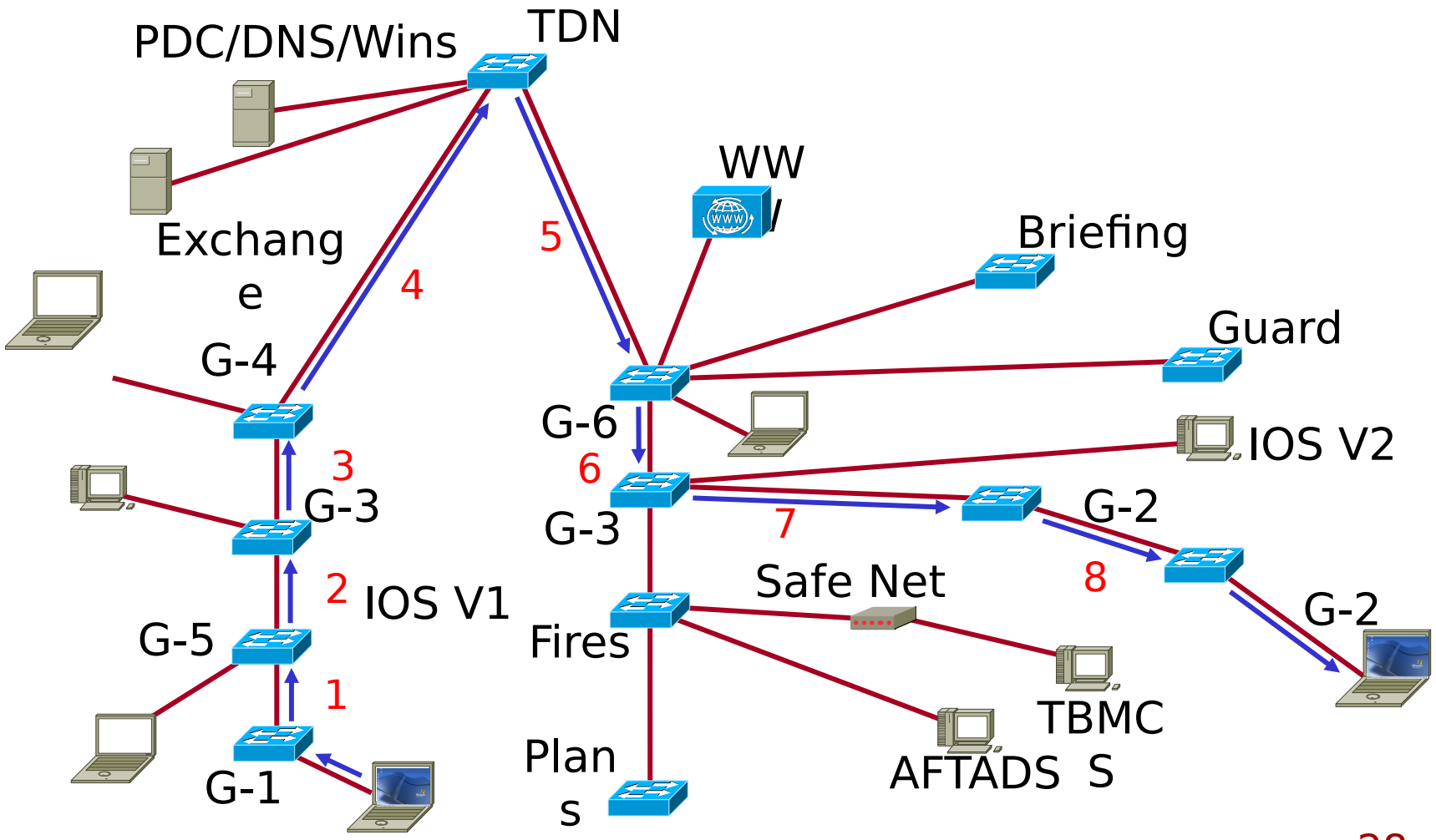
Building Block Method

MSTP



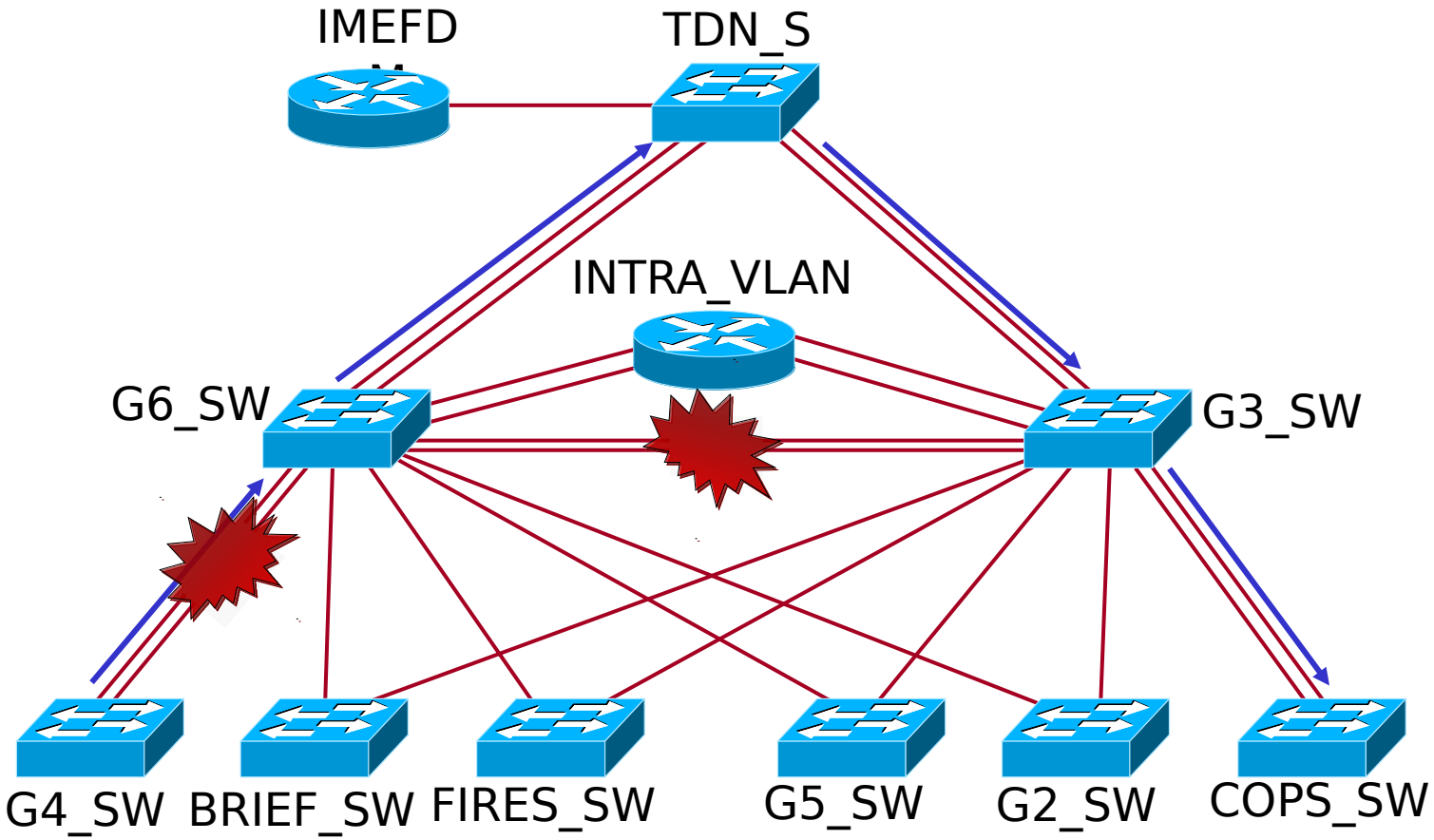
Switching Design

MSTP

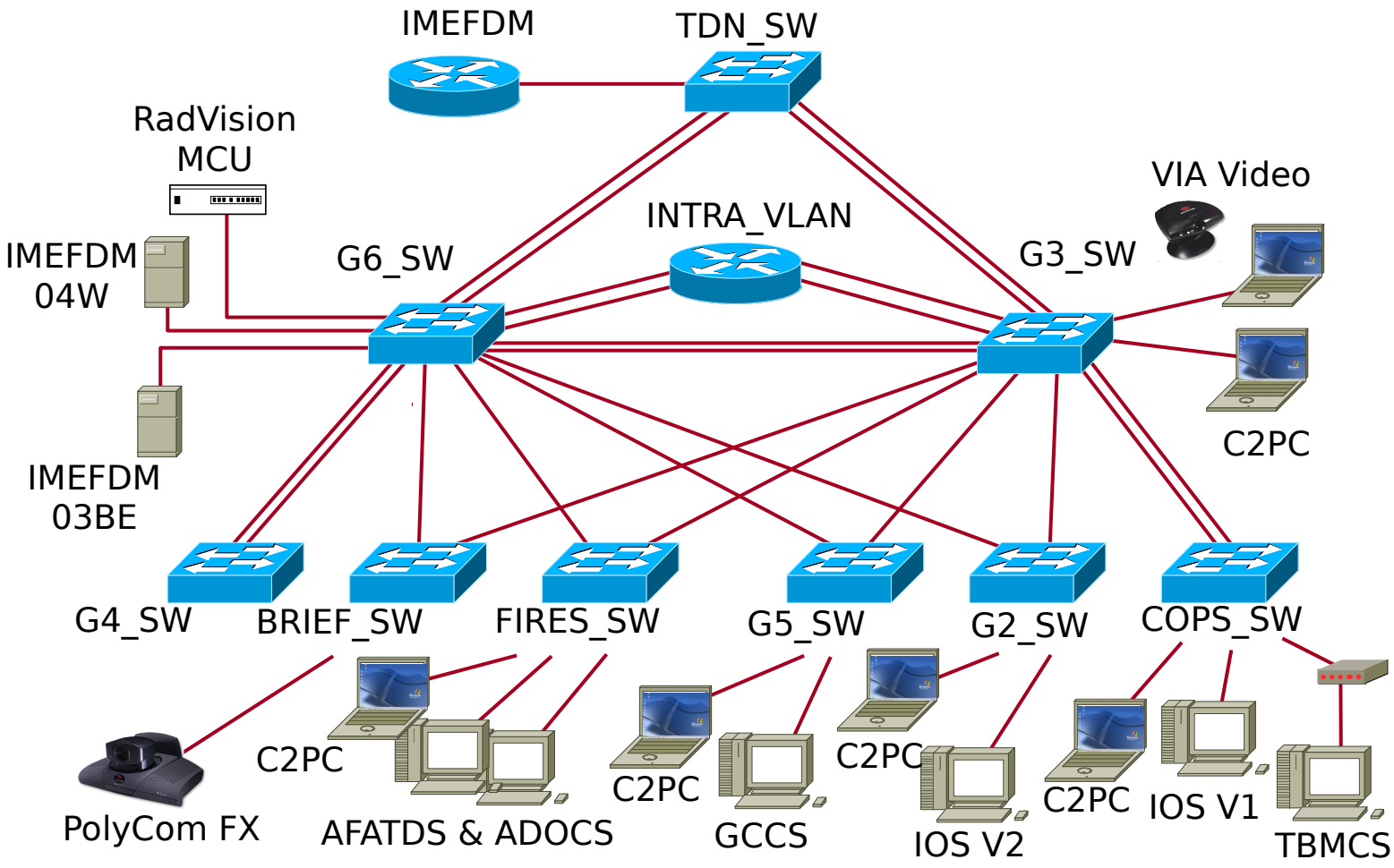


Switching Design (cont.)

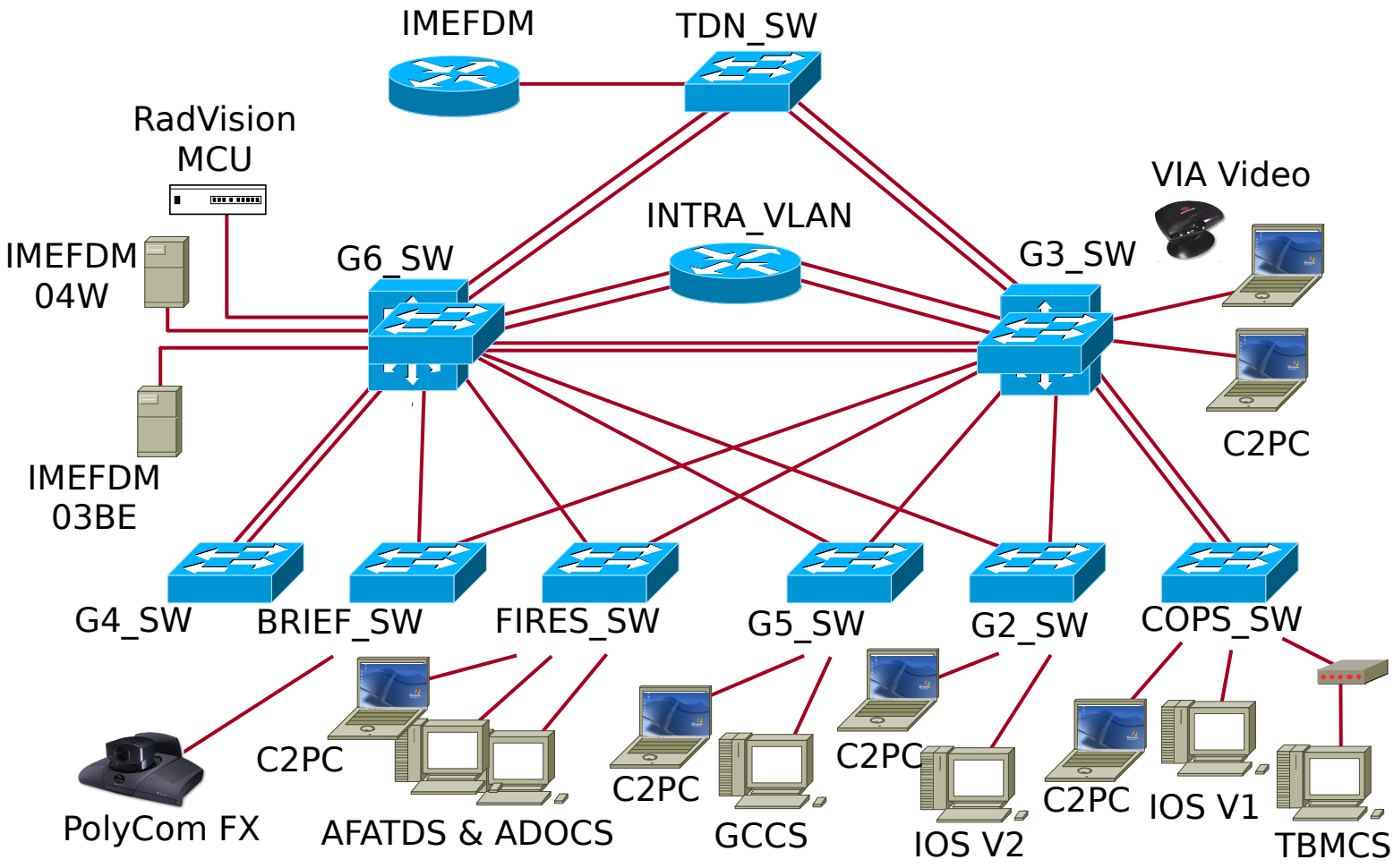
MSTP



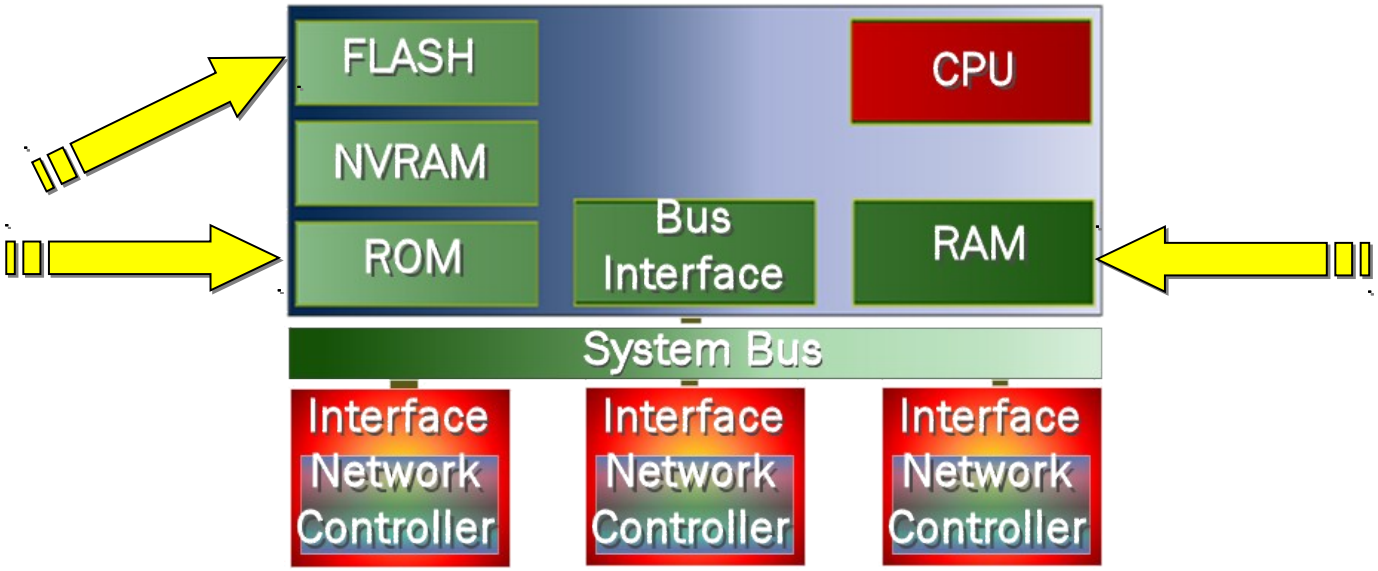
Switching Design (cont.)



Switching Design (cont.)



Switch Hardware



- ROM: Stores the bootstrap program and POST
- FLASH: (EEPROM) holds the Cisco IOS (Inter networking Operating System) holds the switch start-up configuration
- RAM: Provides caching and packet buffering

Flash Files

```
Directory of flash:/


  2  -rwx  976  Mar 3 1993 22:54:09 -05:00
  vlan.dat

  3  drwx  192  Mar 4 1993 05:45:28 -05:00
  c3750-advipservicesk9-mz.122-25.SED1

407  -rwx 2233 Jan 30 2006 19:41:55 -05:00
  config.text


15998976 bytes total (6238208 bytes free)
```

Initial Start-up

- System startup routines initiate switch software
- Initial startup uses default configuration parameters
  - **Before you start the switch, verify the cabling and console connection.**
  - **Attach the power cable plug to the switch power supply socket.**
  - **Observe the boot sequence**
    - **LEDs on the switch chassis**
    - **Cisco IOS software output text**

Command Based CLI

Command Based Switch (29xx, 35xx, 37xx)

- **Switch> [User Exec Mode]**
- **Switch# [Privileged Exec Mode]**
- **Switch(config)# [Global Config Mode]**
- **Switch(config-if)# [Sub-command Mode]**
- **Switch(vlan)# [VLAN Database Mode]**

Set Based CLI

Set Based Switches (4xxx, 5xxx, 55xx, and 6xxx)

- **Switch> [User Exec Mode]**
- **Switch(config)#set xxxxxx xxxxx [Privileged Exec Mode]**

User Exec Commands

- **Switch>**
  - *ping*
  - *show (limited)*
  - *enable*
  - *traceroute*

Privileged Exec Commands

- **Switch#**
  - *All User Exec Commands*
  - *show*
  - *reload*
  - *debug*
  - *configure*

Global Config Commands

Switch (config)#

- *hostname*
- *enable secret*
- *line*
  - *vty*
  - *console*

  → password *cisco*, login
- *interface*
  - *port channel*
  - *fast ethernet*
  - *gigabit ethernet*
  - *vlan*

  → ip address *ip-add subnet-mask*, switchport access vlan [*vlan id*], shutdown / no shutdown
- *router*
  - *rip*
  - *ospf*
  - *igrp*
  - *eigrp*

  → network, version

Configuring the Switch (cont.)

- Lock down the Switch
  - Line Con 0, Line VTY 0 4, and Enable Secret
- Configure the Identity
  - Host name, Services, and Banners
- Configure the VLAN Database
  - VTP Domain and VLANs

Configuring the Switch (cont.)

- Configure Interfaces/Switchports
  - Assign switchports to VLANs and configure Trunks
- Configure Advanced parameters
  - Spanning-Tree
  - HSRP

Step-by-Step

Step #1

Lock Down Switch

```
Switch(config)#line con 0
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#line vty 0 4
Switch(config-line)#password cisco
Switch(config-line)#login
```

Step #1 (cont.)

MSTP

```
Switch(config)#enable secret cisco
Switch(config)#no ip http server
Switch(config)#no ip http secure server
Switch(config)#no ip finger
Switch(config)#no domain-lookup
Switch(config)#service password-encrypt
```

Step-by-Step (cont.)

Step #2

Configure Identity

```
Switch(config)#clock timezone EST -5 +9

Switch(config)#end

Switch#clock set 16:27:00 22 May 2005

Switch(config)#hostname IMEF_S1

IMEF_S1(config)#service timestamps debug
datetime localtime show-timezone

IMEF_S1(config)#service timestamps log
datetime localtime show-timezone

IMEF_S1(config)#banner motd ^  TEXT  ^
```

Step #2 (cont.)

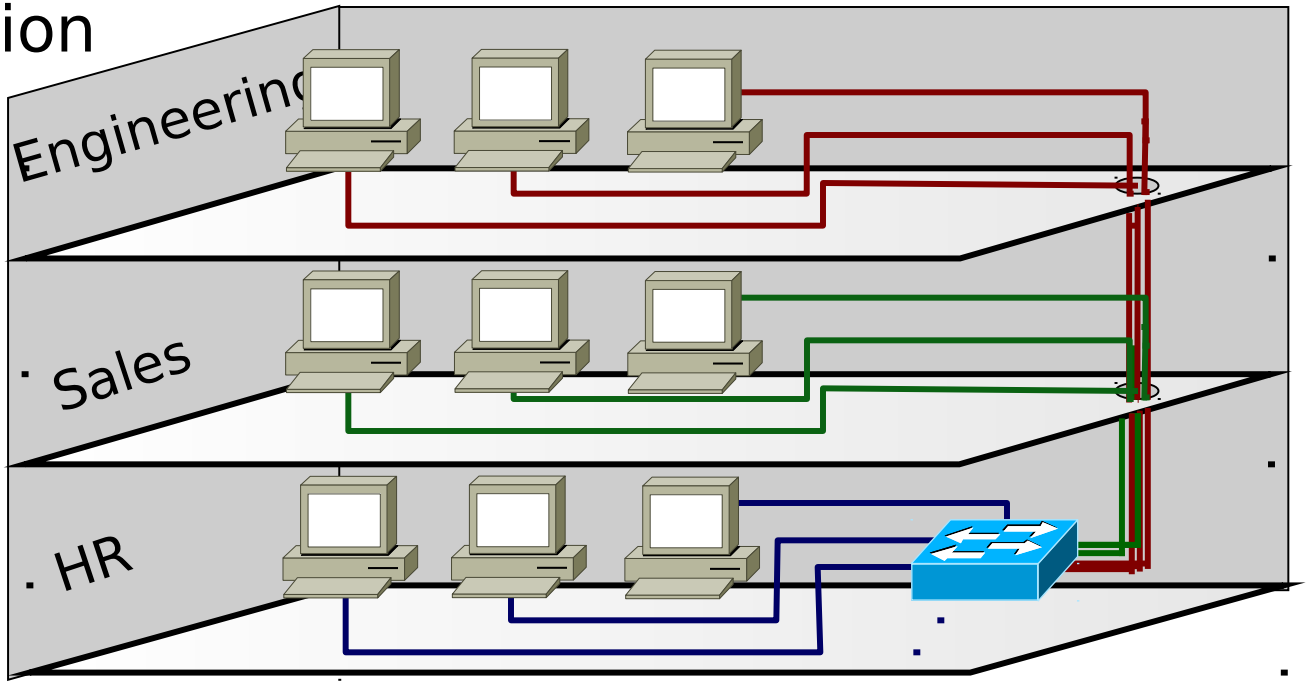

```
IMEF_S3(config)#interface VLAN 102
IMEF_S3(config-if)#ip add <add> <mask>
IMEF_S3(config-if)#exit
IMEF_S3(config)#ip default-gat A.B.C.D
IMEF_S3(config)#snmp-serv comm pub ro
```

Lab #1

Lock Down Switch & Configure Identity

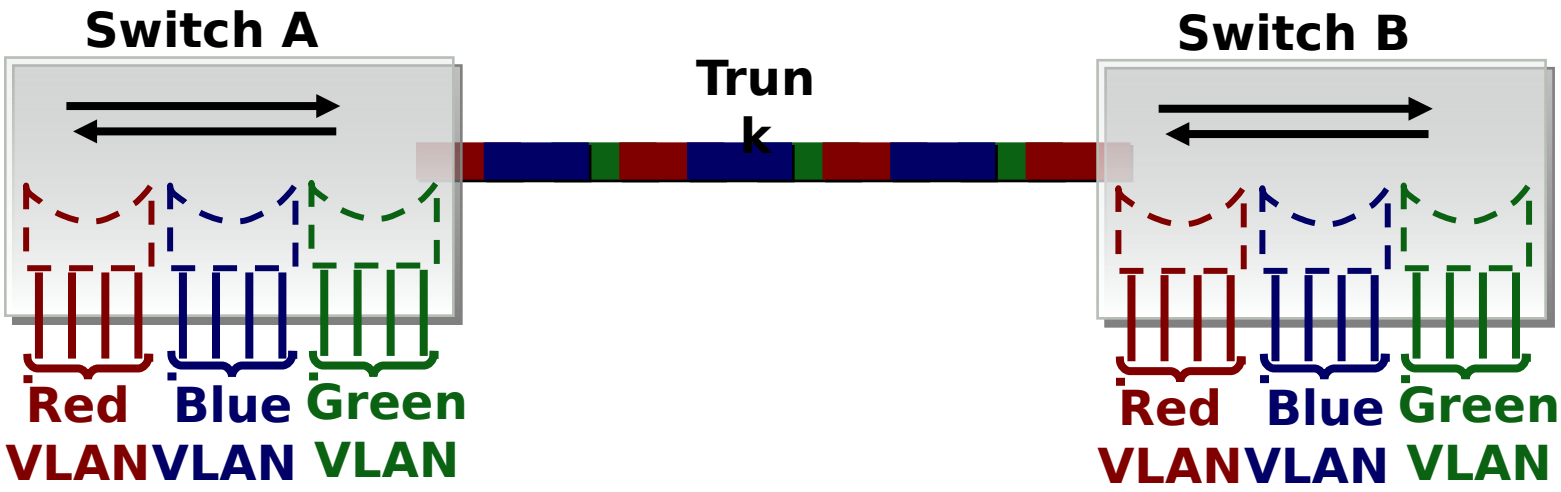
VLANs

- Segmentation
- Flexibility
- Security



A VLAN = A broadcast domain = Logical network (subnet)

VLAN Operations



- Each logical VLAN is like a separate physical bridge
- VLANs can span across multiple switches
- Trunks carry traffic for multiple VLANs

VLAN Specs

- Maximum number of VLANs, switch-dependent
  - VTP ISL Protocol, support 1,024 VLANS
  - VTP DOT1Q Protocol supports 4,096 VLANs
- 5 Factory Default VLANS
  - VLAN 1 (Can not change VLAN 1 name)
  - VLAN 1001-1005
- CDP and VTP advertisements sent on VLAN1
  - Must be in VTP *server* or *transparent* mode to create, add, or delete VLANs

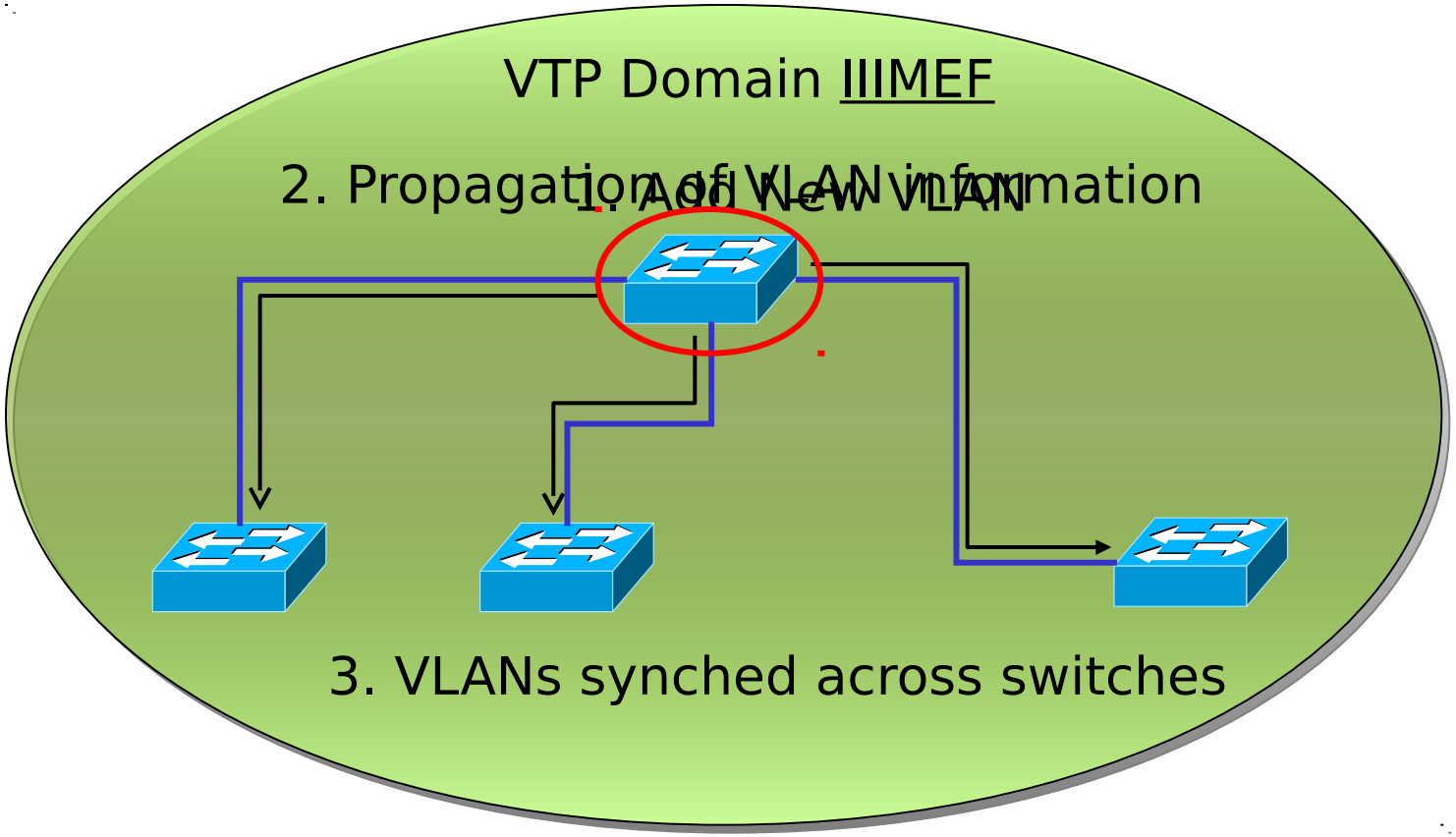
Configuring VLANs

- Enable VTP (optional)
- Enable trunking
- Create VLANs
- Assign VLAN to ports

VLAN Trunking Protocol (VTP)

- A messaging system that advertises VLAN configuration information
- Maintains VLAN configuration consistency throughout a common administrative domain
- VTP sends advertisements on trunk ports only
- Support mixed media trunks (Fast Ethernet, FDDI, ATM)

VLAN Trunking Protocol (VTP)



VTP Modes

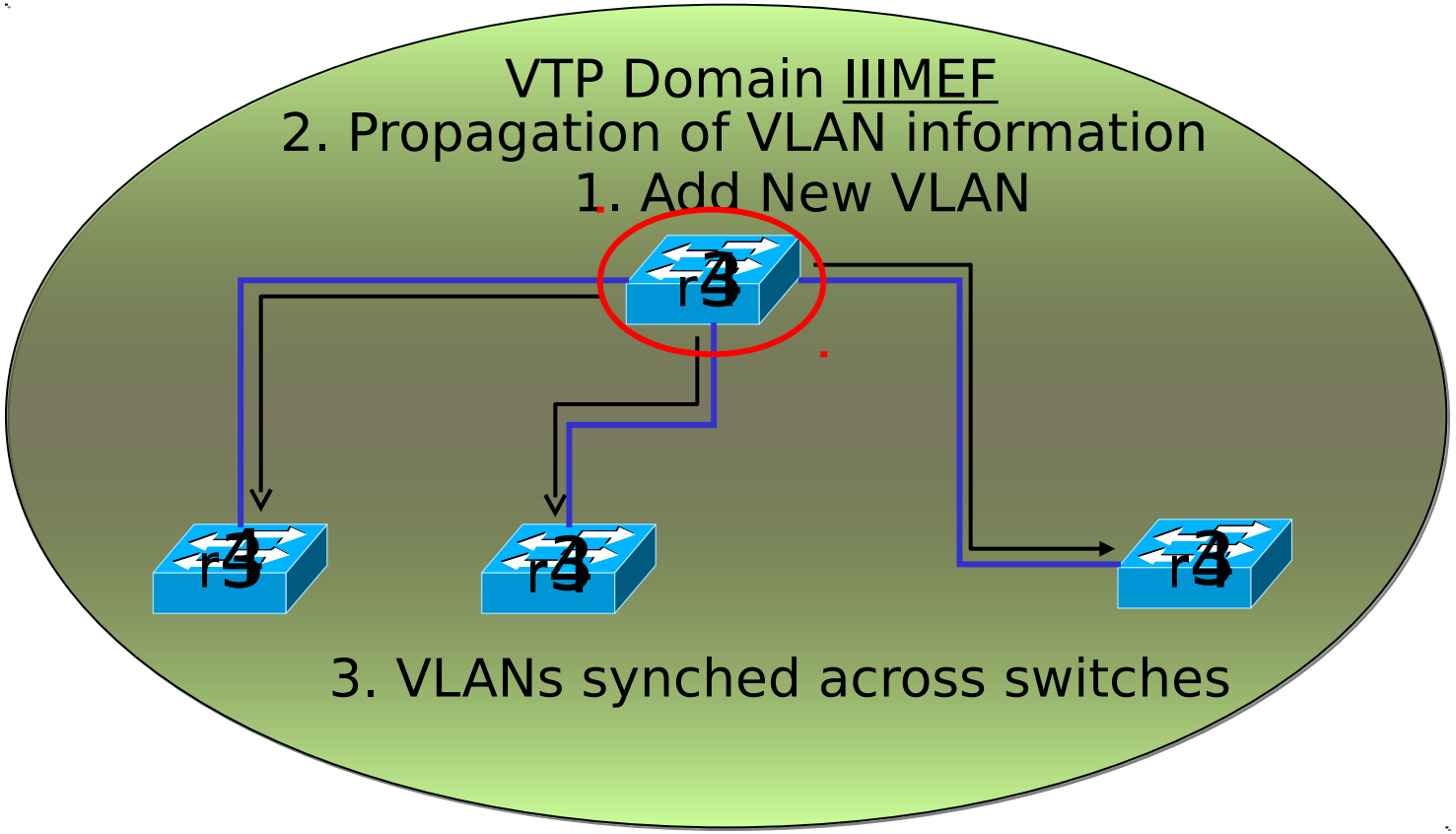
MSTP

Transparent

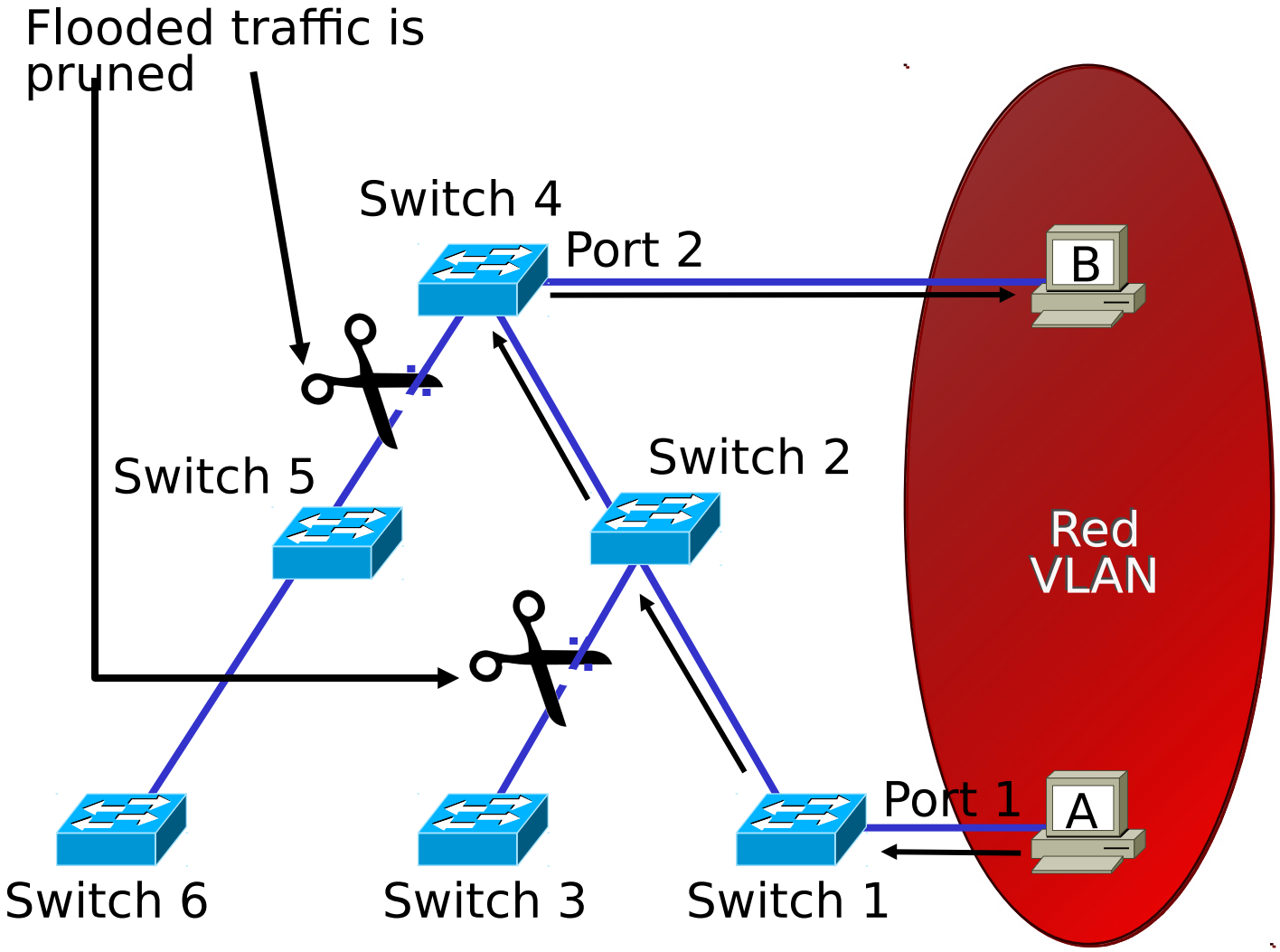
Transparent Mode

- Forwards VTP Advertisements
- Does not synchronize Domain and VLAN information
- Saved in NVRAM

VTP Process


VTP Domain IIIMEF
2. Propagation of VLAN information
1. Add New VLAN
3. VLANs synched across switches

VTP Pruning


Flooded traffic is pruned
Switch 4
Port 2
B
Switch 5
Switch 2
Red VLAN
Port 1
A
Switch 6
Switch 3
Switch 1

VTP Configuration

- VTP domain name
- VTP mode
- VTP pruning
- VTP password

Use caution when adding a new switch into an existing domain. A new switch should be added in client mode to prevent the new switch from propagating incorrect VLAN information.

VTP Status


```
3750_2nd_Un#show vtp status
VTP Version                     : 2
Configuration Revision          : 80
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 17
VTP Operating Mode              : Client
VTP Domain Name                 : MSTP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x67 0xF8
0xF9 0x91 0x20 0xC1 0x03 0x45
```

Adding a VLAN


```
IMEF_SW1#vlan data
IMEF_SW1(vlan)#vlan 9 name
IMEF_SW1(vlan)#
                exit

IMEF_SW1(config)#
IMEF_SW1(config-vlan)#vlan 102
IMEF_SW1(config-vlan)#name
IMEF_SW1(config-vlan)#
IMEF_SW1(config-vlan)#vlan 103
IMEF_SW1#               name Servers
                        end
```

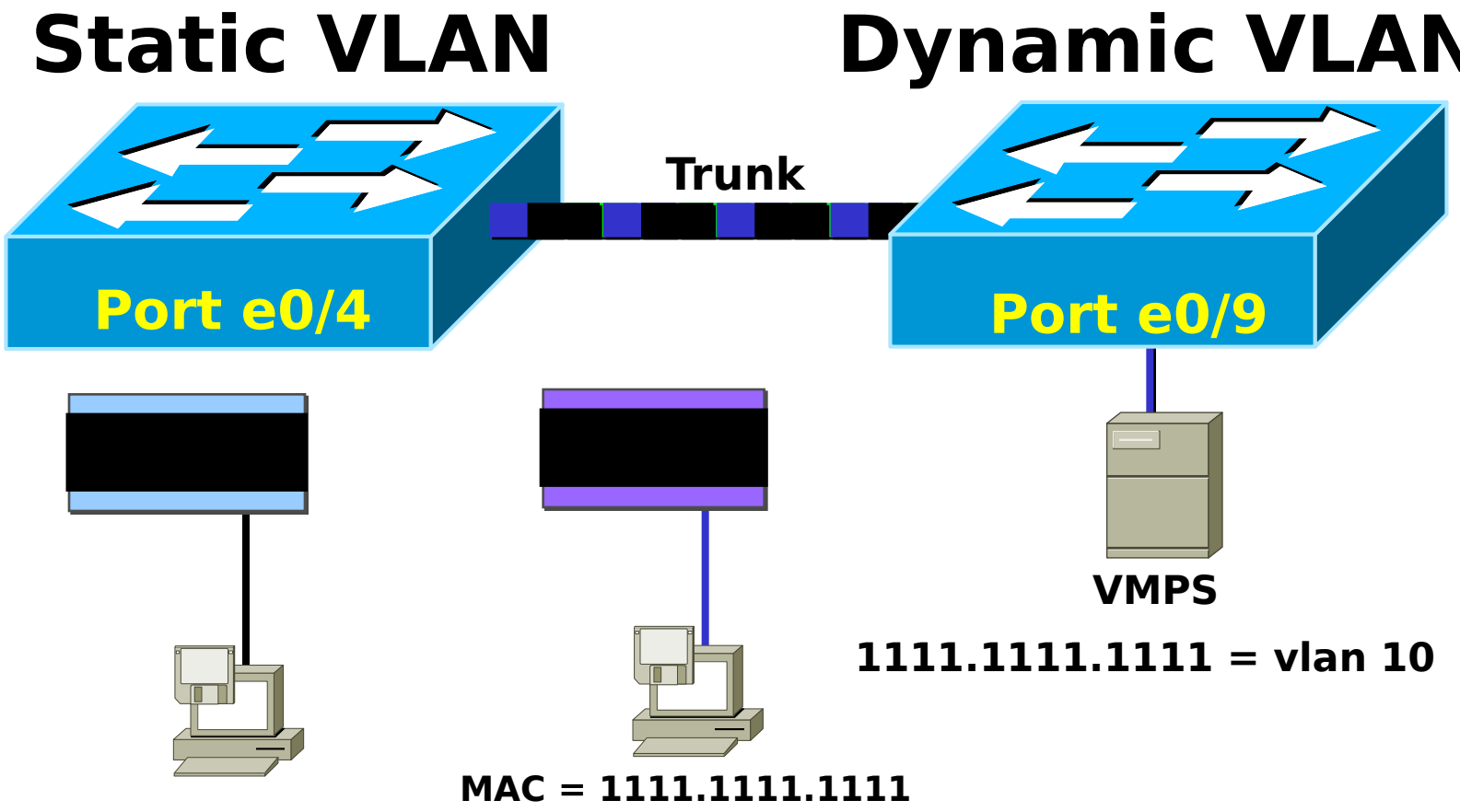
Verifying a VLAN


```
3550-B-Unc#sho vlan id 3

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
3    138.156.165.0                       active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                                   Gi0/5, Po1

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1
   Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ --
3    enet  100003     1500  -      -      -        -    -        0      0
```

Verifying a VLAN (cont.)


```
3550-B-Unc#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -----
1    default                             active    Gi0/6
2    138.156.24.0/24                     active
3    138.156.165.0/24                    active
102  138.156.119.0/24                    active
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup
```

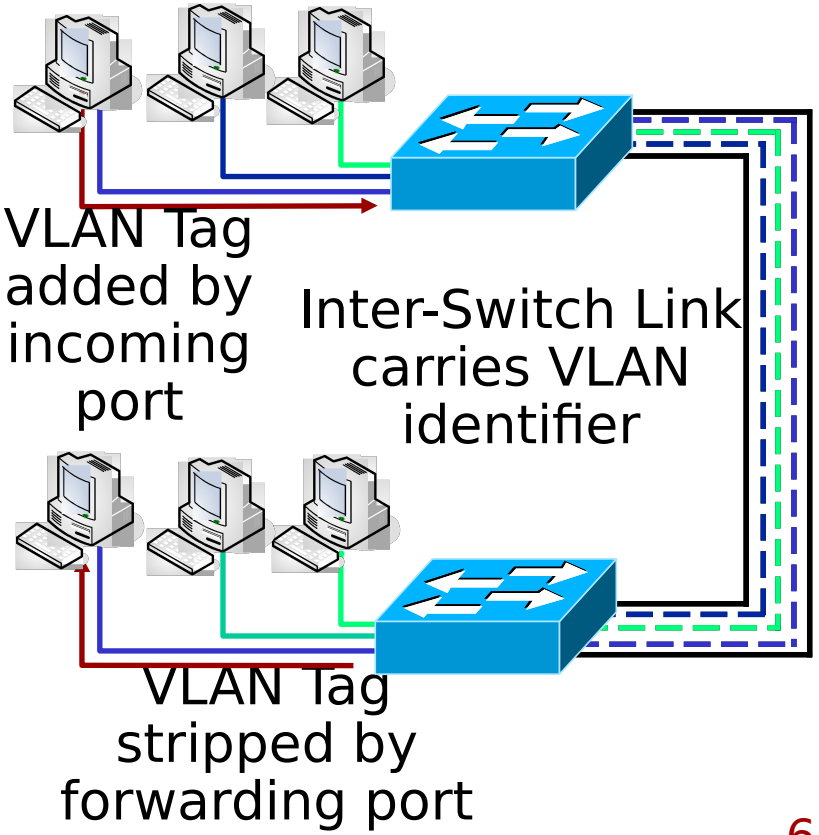
VLAN Membership Modes



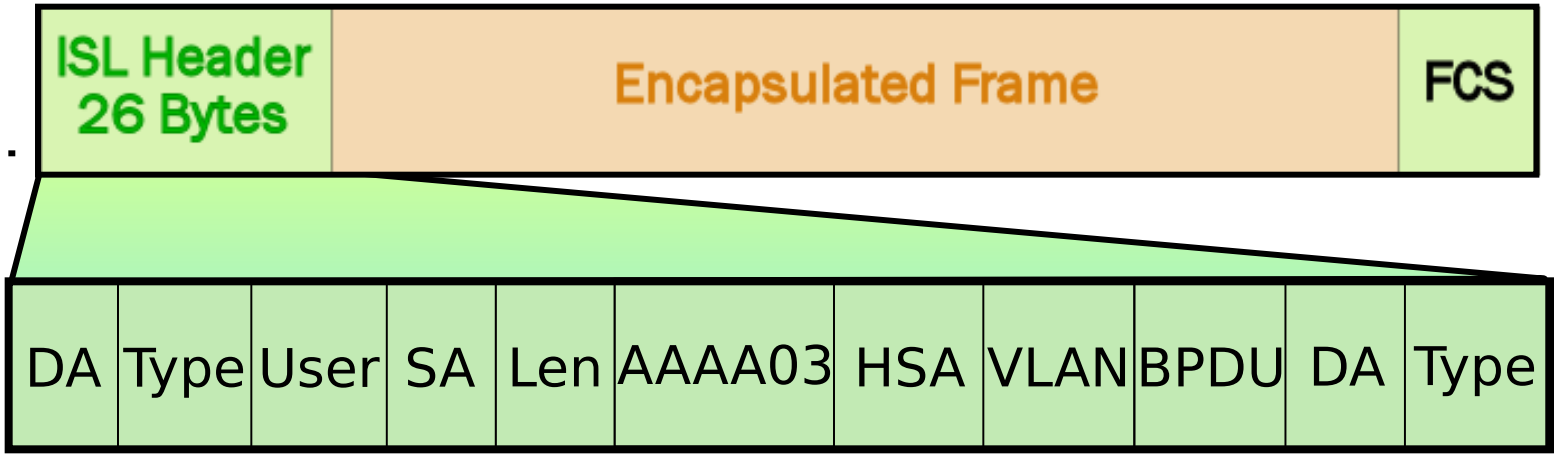
ISL Encapsulation

ISL trunks enable VLANs across a backbone

- Performed with application-specific integrated circuits (ASIC)
- Not intrusive to client stations; client does not see the ISL header
- Effective between switches, routers and switches, and switches and servers with ISL NICs



ISL Encapsulation



- Frames encapsulated with ISL header and CRC
- Support for 1,024 VLANs
- VLAN field (10 Bits)
- BPDU bit
- Can Exceed 1518 bytes results in Large frames called “Giants”.
- VTP can handle these larger frames

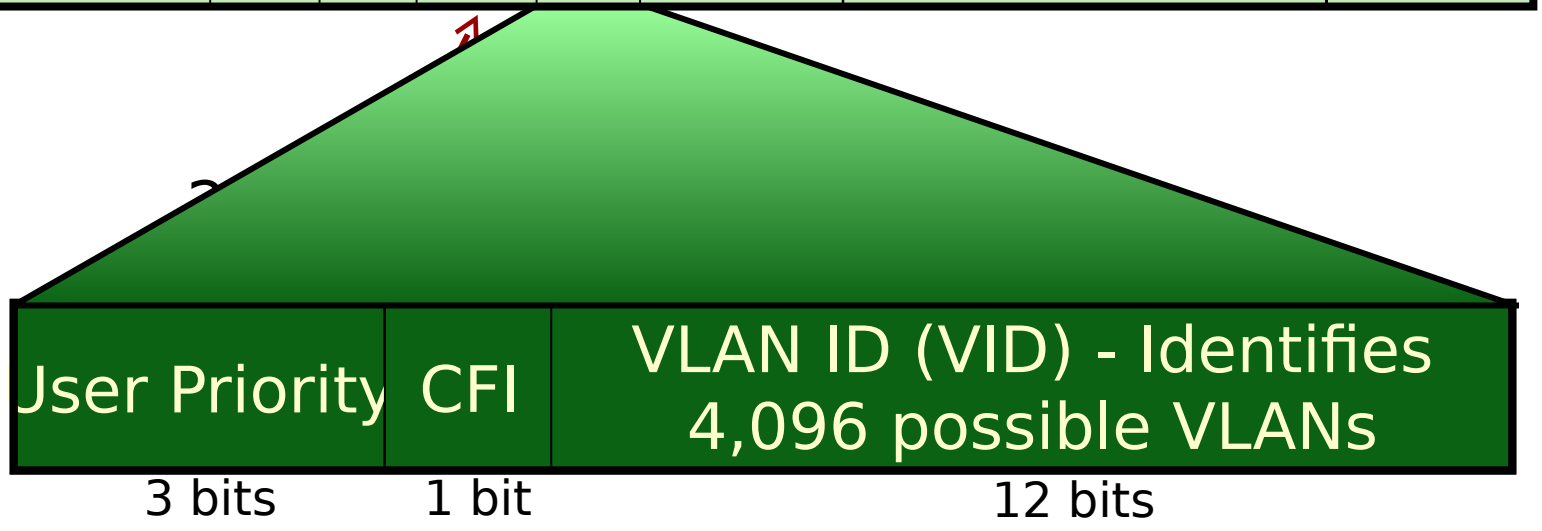
802.1Q

Normal Ethernet Frame

Preamble	Dest. Address	Source Address	Type/ Length	Data	CRC:4

802.1Q Frame

Preamble	DA	SA	2 TPI	2 TAG	Type/ Length	Data	CRC:4



Show Interface


```
3550-B-Unc# show interface gigabit 0/2 switchport
Name: Gi0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
```

Show Interface (cont.)


```
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
3550-B-Unc#
```

Step by Step (cont.)

Step #3 Configure VLAN Database

```
IMEF_S2(config)#vtp mode server
IMEF_S2(config)#vtp domain IMEF
IMEF_S2(config)#vlan 103
IMEF_S2(config-vlan)#name Servers

 OR    Used on older IOS's

IMEF_S2#vlan database
IMEF_S2(vlan)#vlan 103 name Servers
IMEF_S2(vlan)#exit
```

Step-by-Step (cont.)

Step #4. Configure Interfaces & Switchports

```
IMEF_S4(config)#interface fa 0/12
IMEF_S4(config-if)#switch acc vlan 107
IMEF_S2(config)#int fa 1/0/1
IMEF_S2(config-if)#des Trunk to S1
IMEF_S2(config-if)#swi trun encap dot1q
IMEF_S2(config-if)#switch mode trunk
```

Lab #2

Configure Switchports
&
Configure Trunks

Lab #3

Configure VTP
&
Configure VLANs

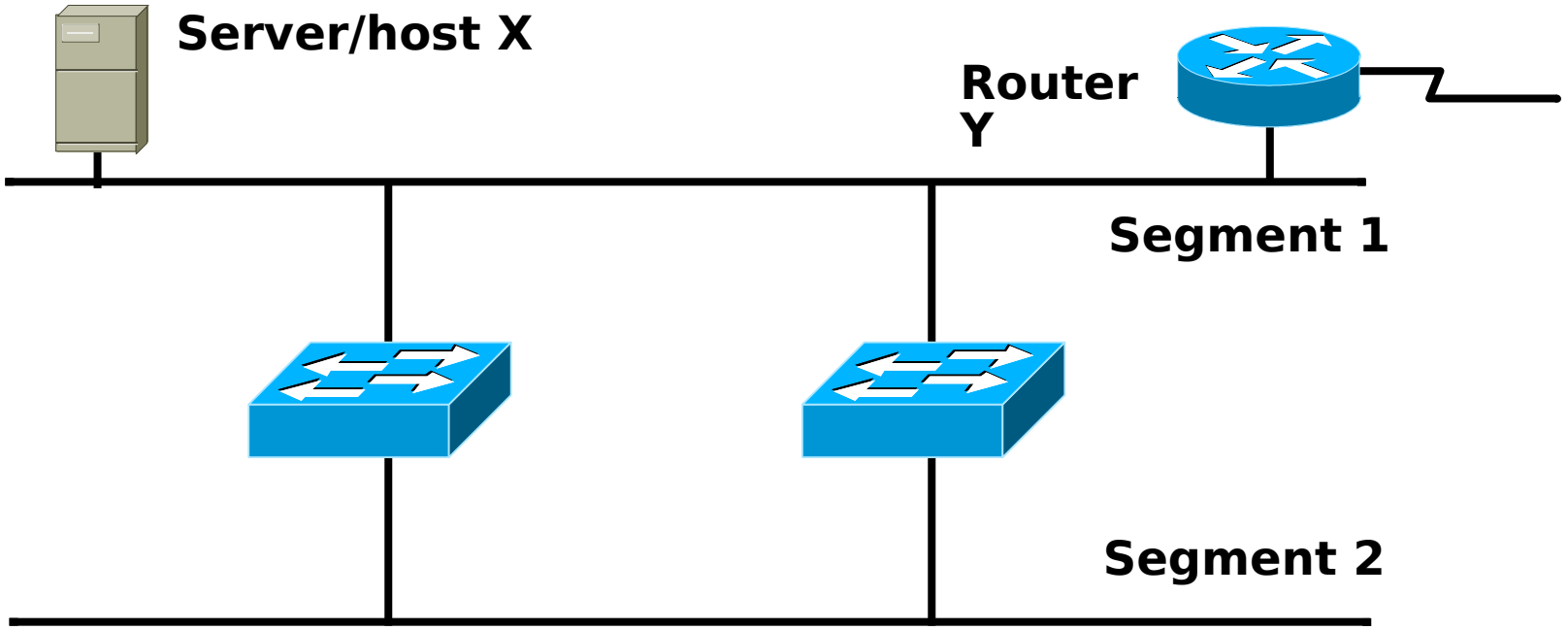
Advanced Configuration

MSTP

Step #5 Configure Advanced Parameters

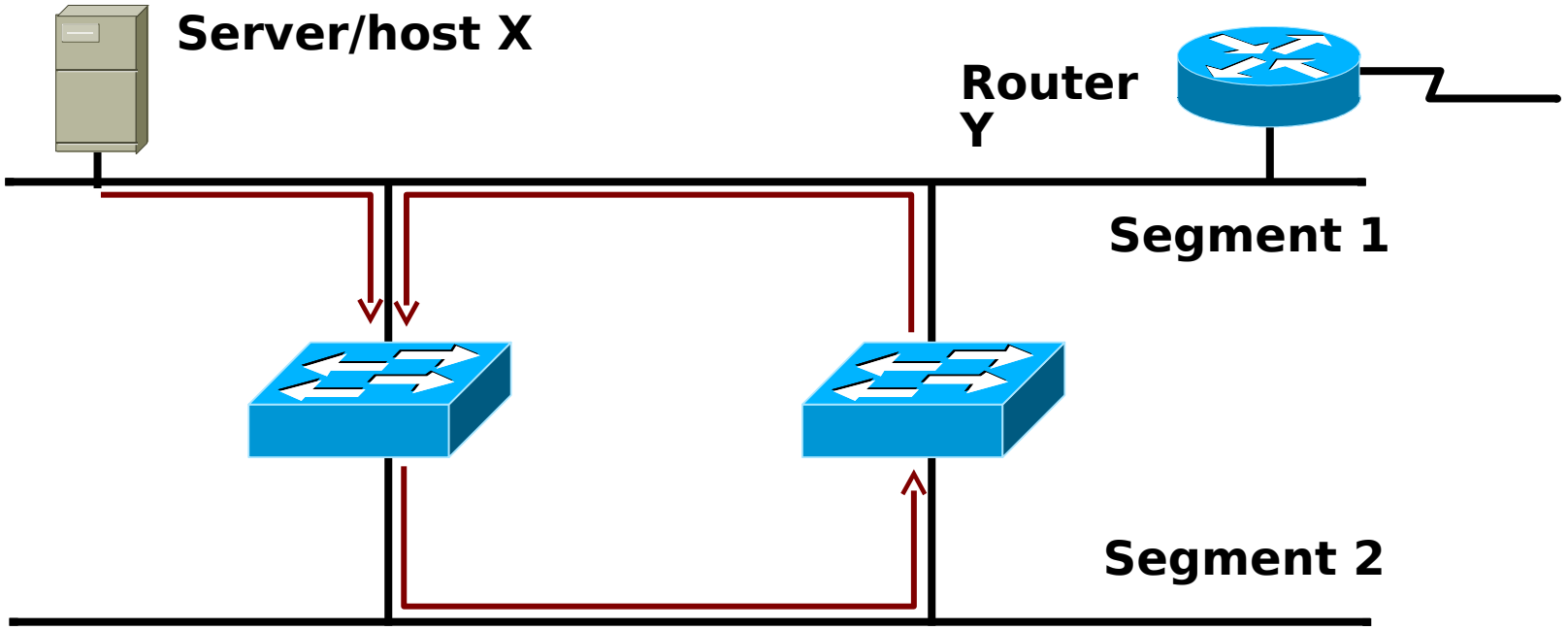
- Spanning Tree
  - Root Switch/Bridge
  - Per VLAN Spanning Tree
  - Command based v/s Set Based CLI
- Port-Channels
- Hot Standby Routing Protocol (HSRP)

Redundancy



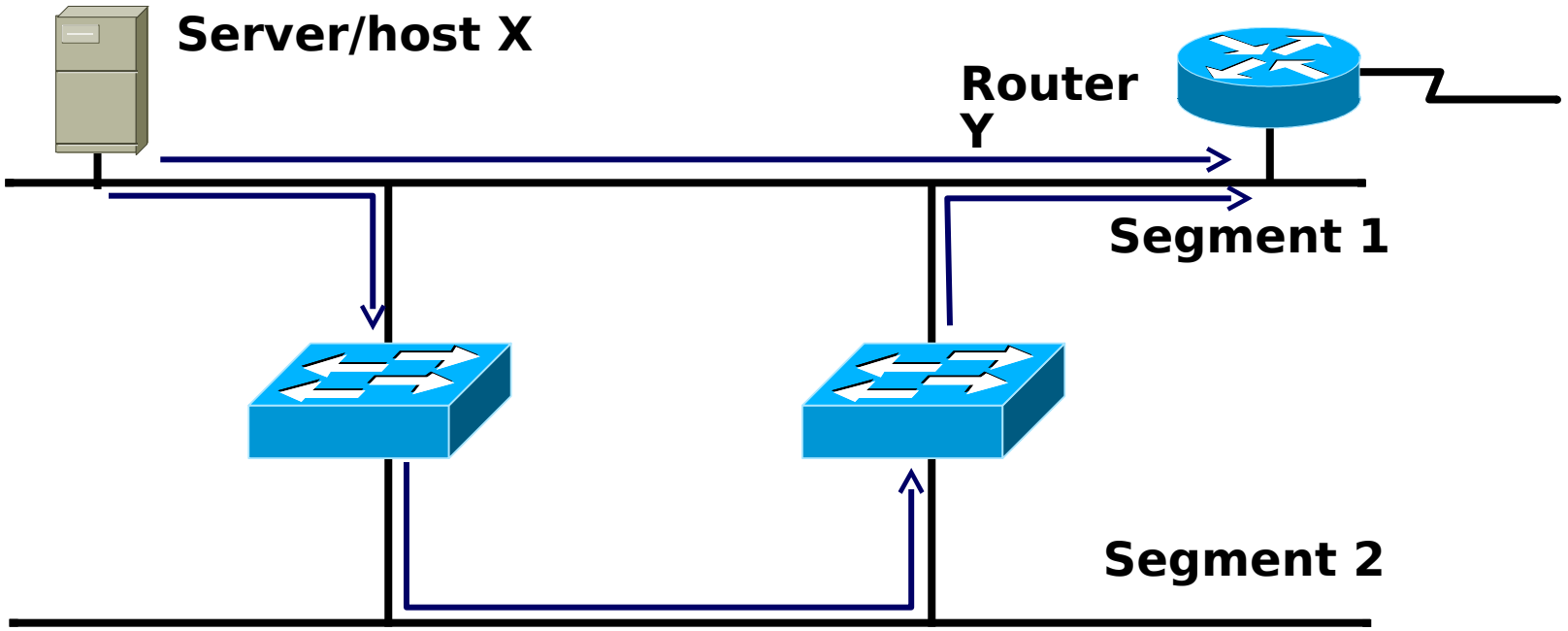
- Redundant topology eliminates single points of failure
- Redundant topology causes broadcast storms, multiple frame copies, and MAC address table instability problems

Broadcast Storms



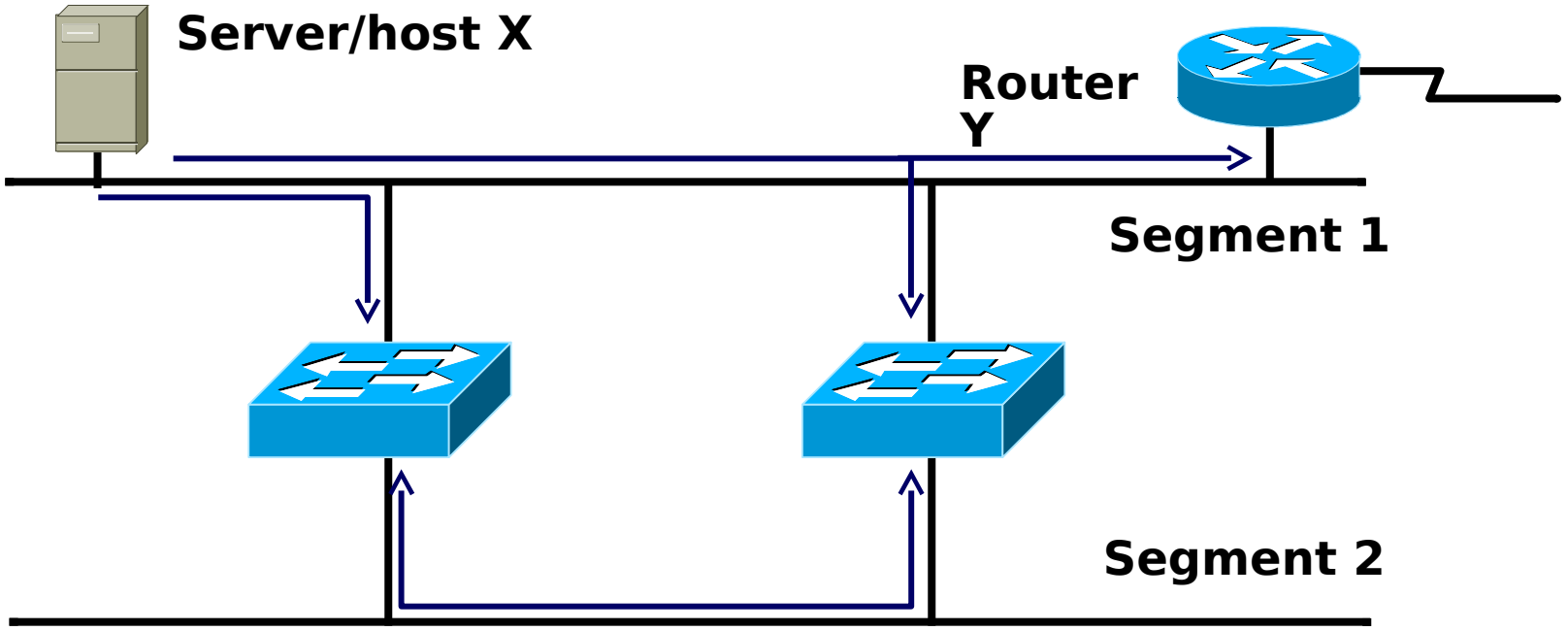
- Host X sends a broadcast
- Switches continue to propagate broadcast traffic

Multiple Frame Copies



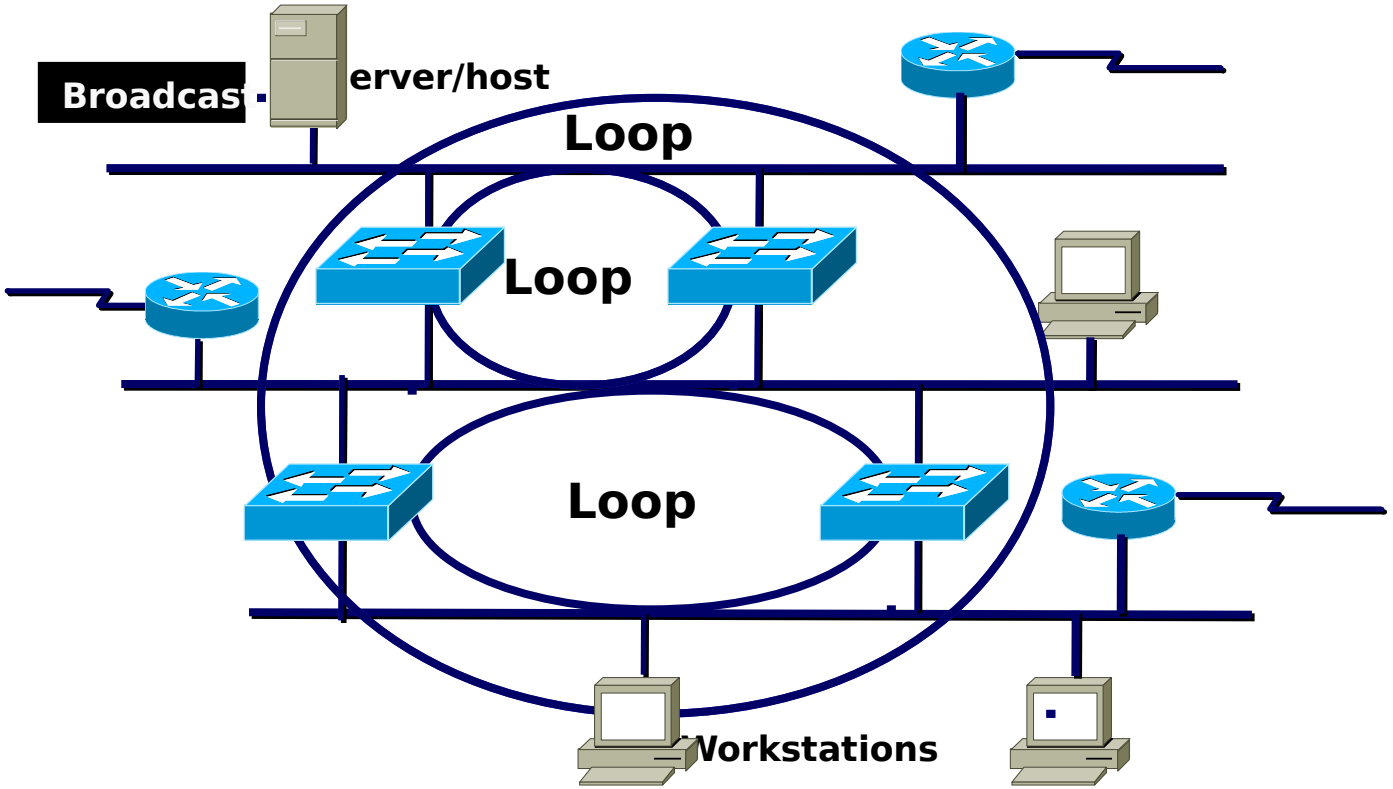
- Host X sends a unicast frame to Router Y
- Router Y MAC Address has not been learned by either Switch yet
- Router Y will receive two copies of the same frame

MAC Address Instability



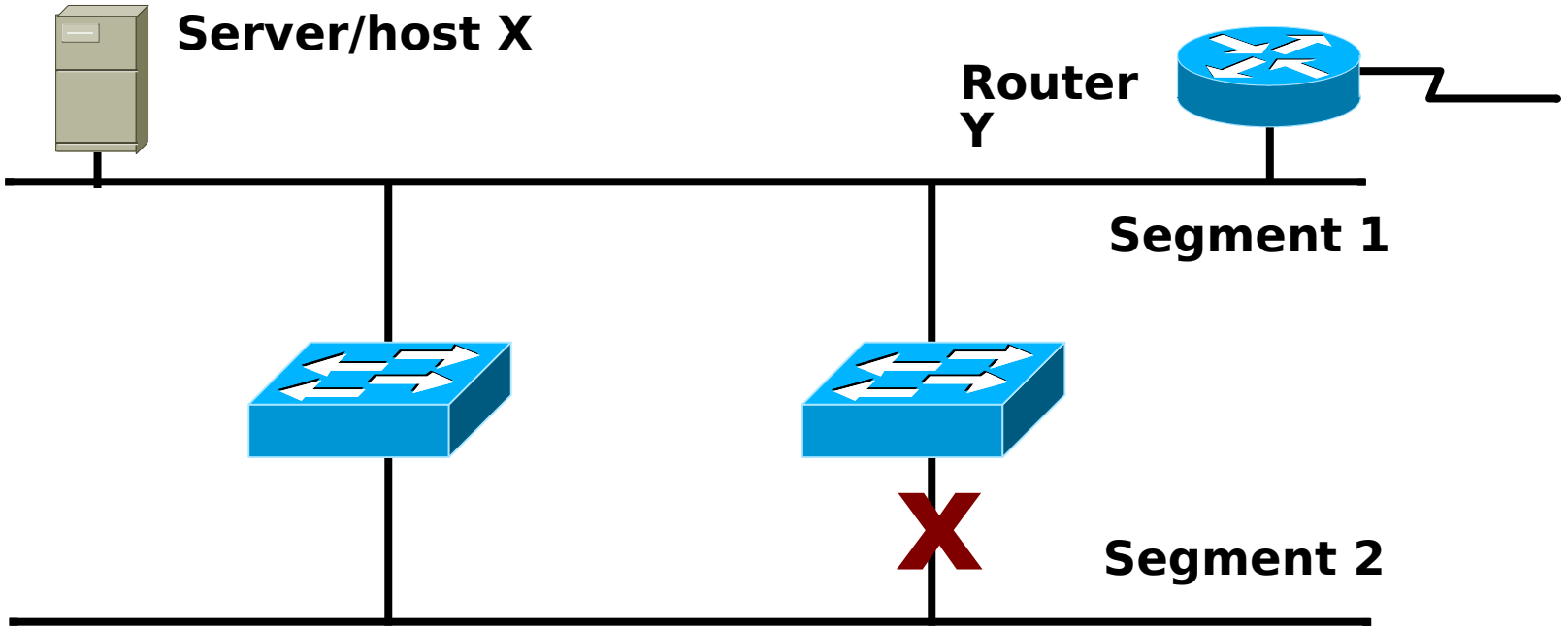
- Host X sends a unicast frame to Router Y
- Router Y MAC Address not learned by Switches yet
- Switch A and B learn Host X MAC address on port 0
- Frame to Router Y is flooded
- Switch A and B learn Host X MAC address on port 1

Multiple Loop Problems



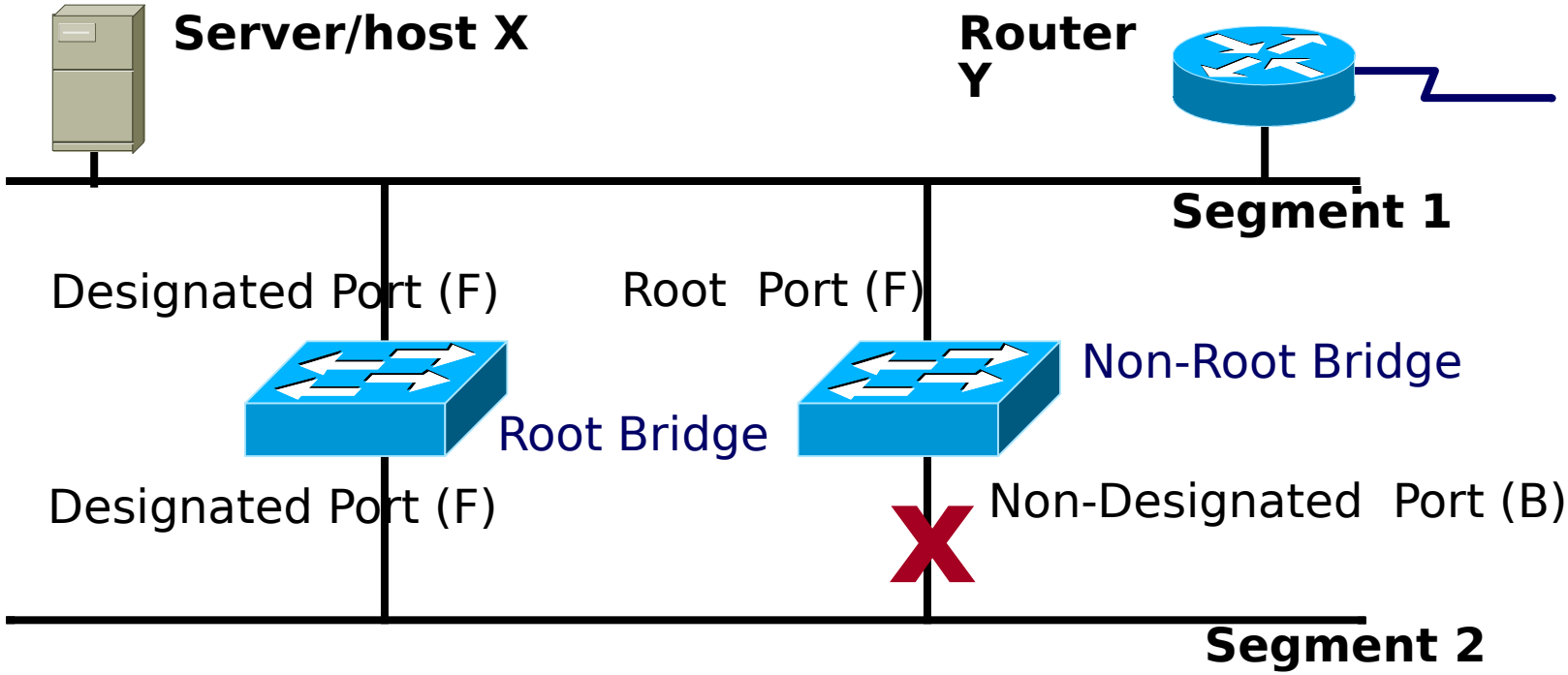
- Complex topology can cause multiple loops to occur
- Layer 2 has no mechanism to stop the loop

Spanning Tree



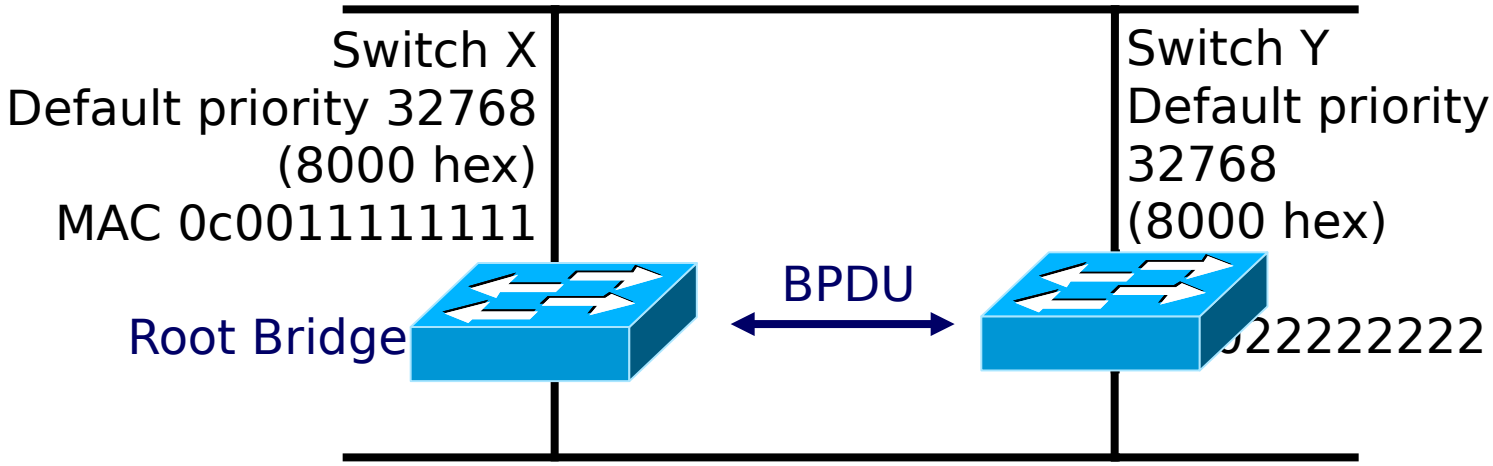
Provides a loop free redundant network topology by placing certain ports in the blocking state

Spanning Tree (cont.)



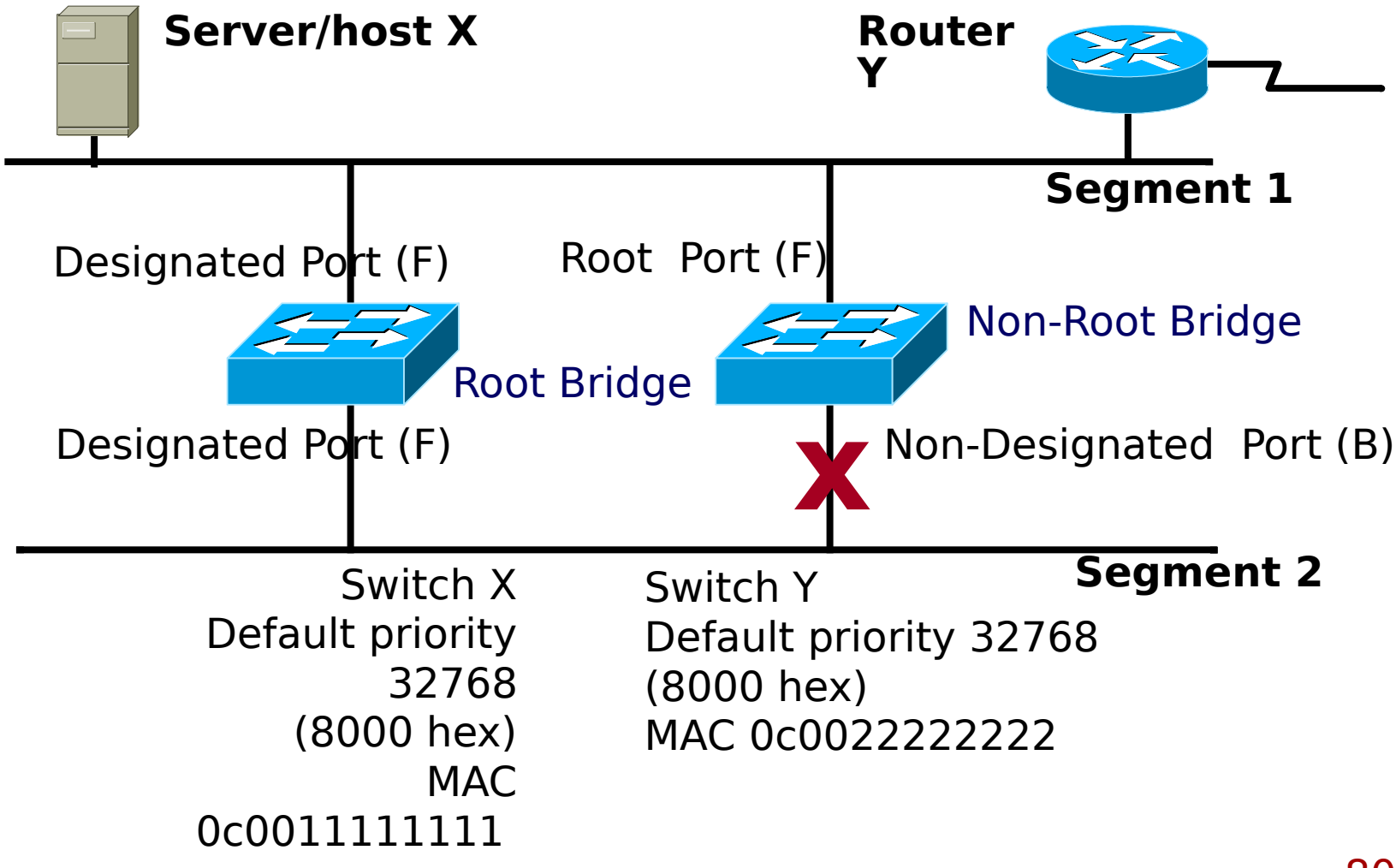
- One root bridge per network
- One root port per nonroot bridge
- One designated port per segment

Root Bridge Selection



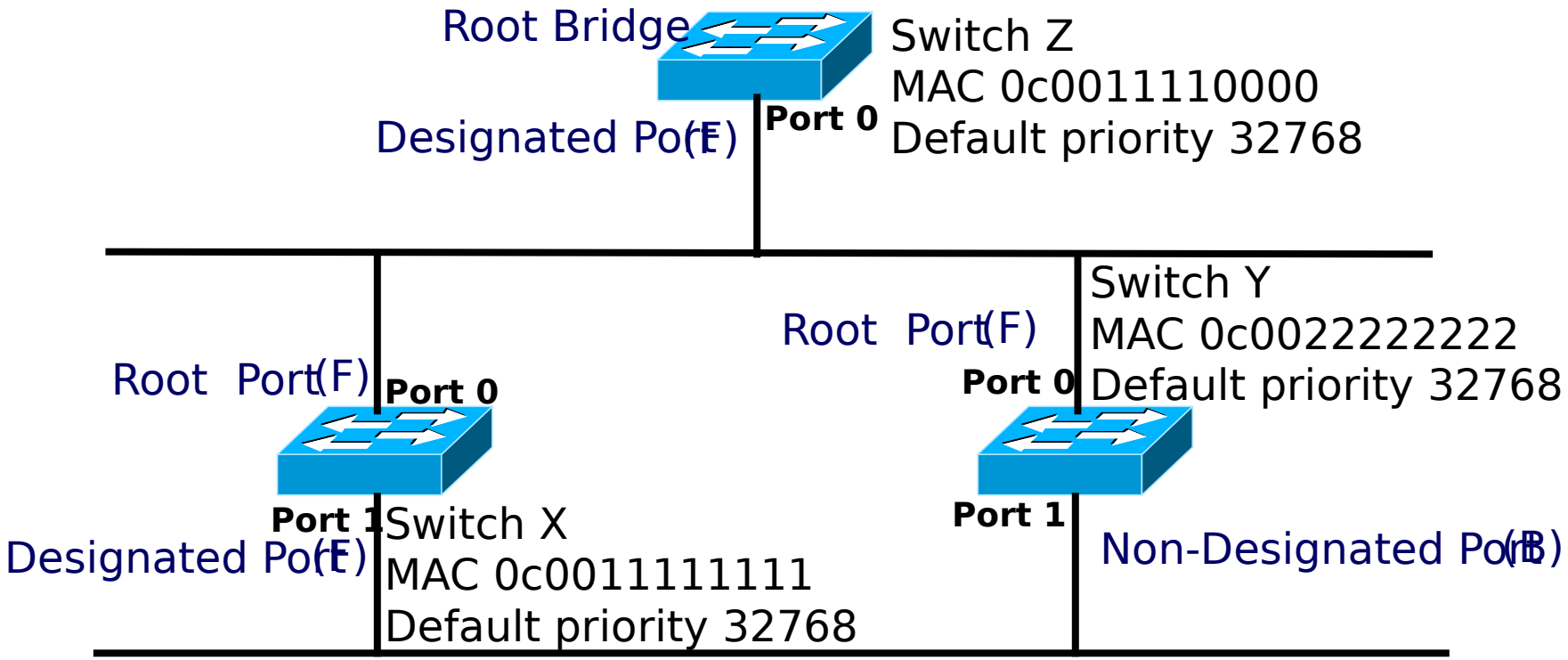
- BPDU = Bridge protocol data unit
  (default = sent every 2 seconds)
- Root bridge = Bridge with the lowest bridge ID
- Bridge ID = Bridge priority + bridge MAC address
- Which switch has the lowest bridge ID?

Port States


Server/host X
Router Y
Segment 1
Designated Port (F)
Root Port (F)
Non-Root Bridge
Root Bridge
Designated Port (F)
Non-Designated Port (B)
X
Segment 2
Switch X
Default priority
32768
(8000 hex)
MAC
0c0011111111
Switch Y
Default priority 32768
(8000 hex)
MAC 0c0022222222

Spanning-Tree

MSTP



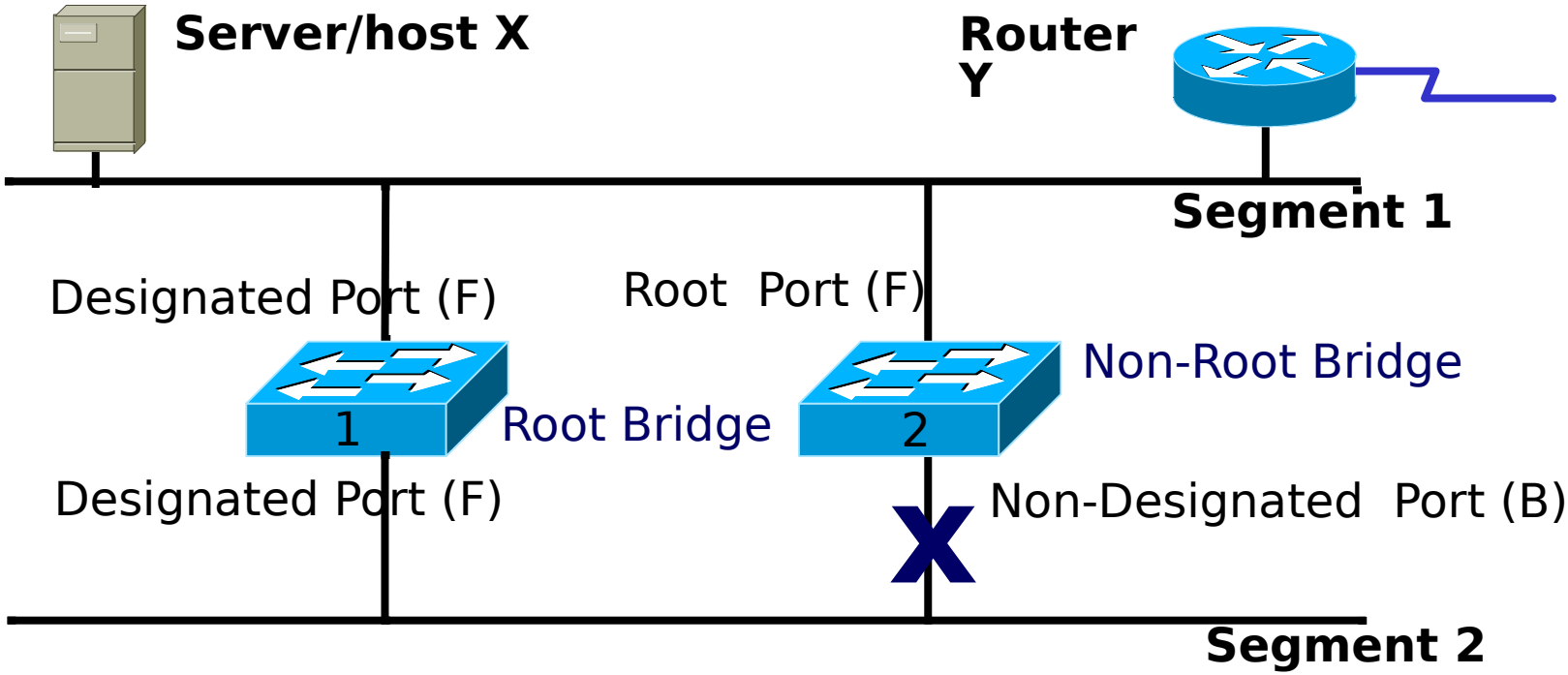
- Which is the root bridge?
- Label the root, designated & non-designated ports?
- Which are the forwarding & blocking ports?

Port States

Spanning-tree transitions each port through several different states:

- Blocking
- Listening
- Learning
- Forwarding

Spanning Tree



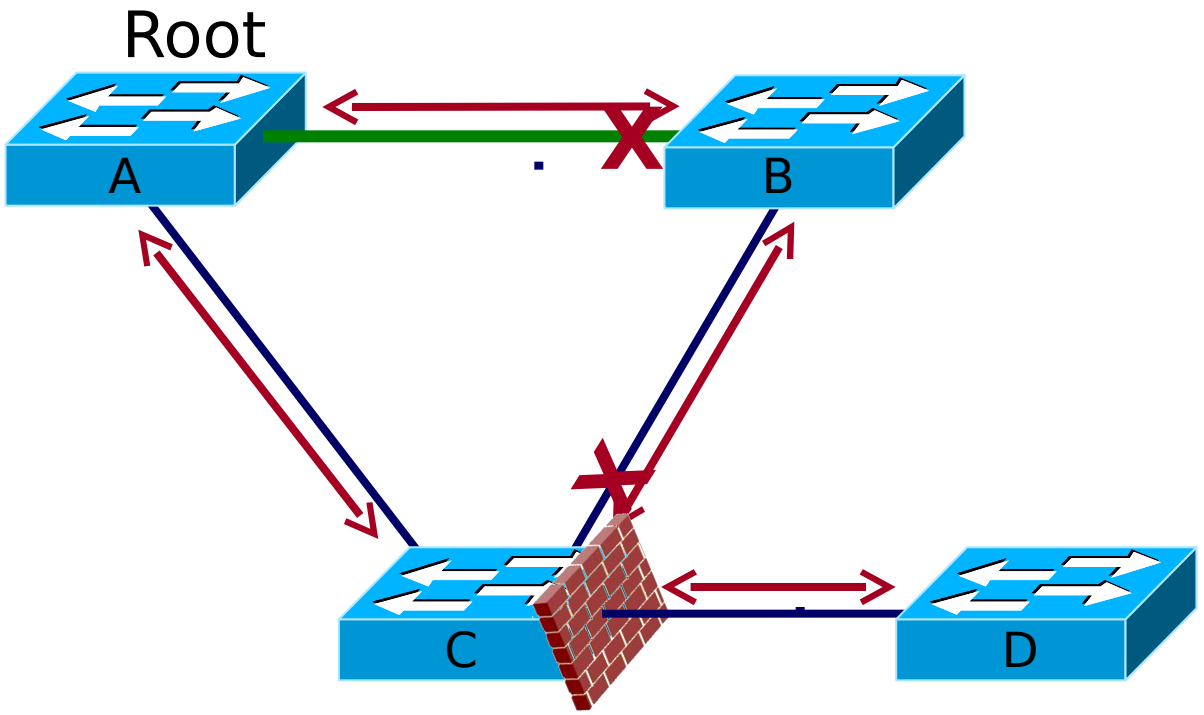
Convergence

- Convergence occurs when all the switches and bridge ports have transitioned to either the forwarding or blocking state.
- When network topology changes, switches and bridges must re-compute the Spanning-Tree Protocol, which disrupts user traffic.

Advanced STP

- Portfast
  - Allows immediate transition of the port into forwarding state. PortFast immediately transitions the port into STP forwarding mode upon linkup.
- Portfast BPDU guard
  - At the reception of BPDUs, the BPDU guard operation disables the port that has PortFast configured.

Advanced STP (cont.)

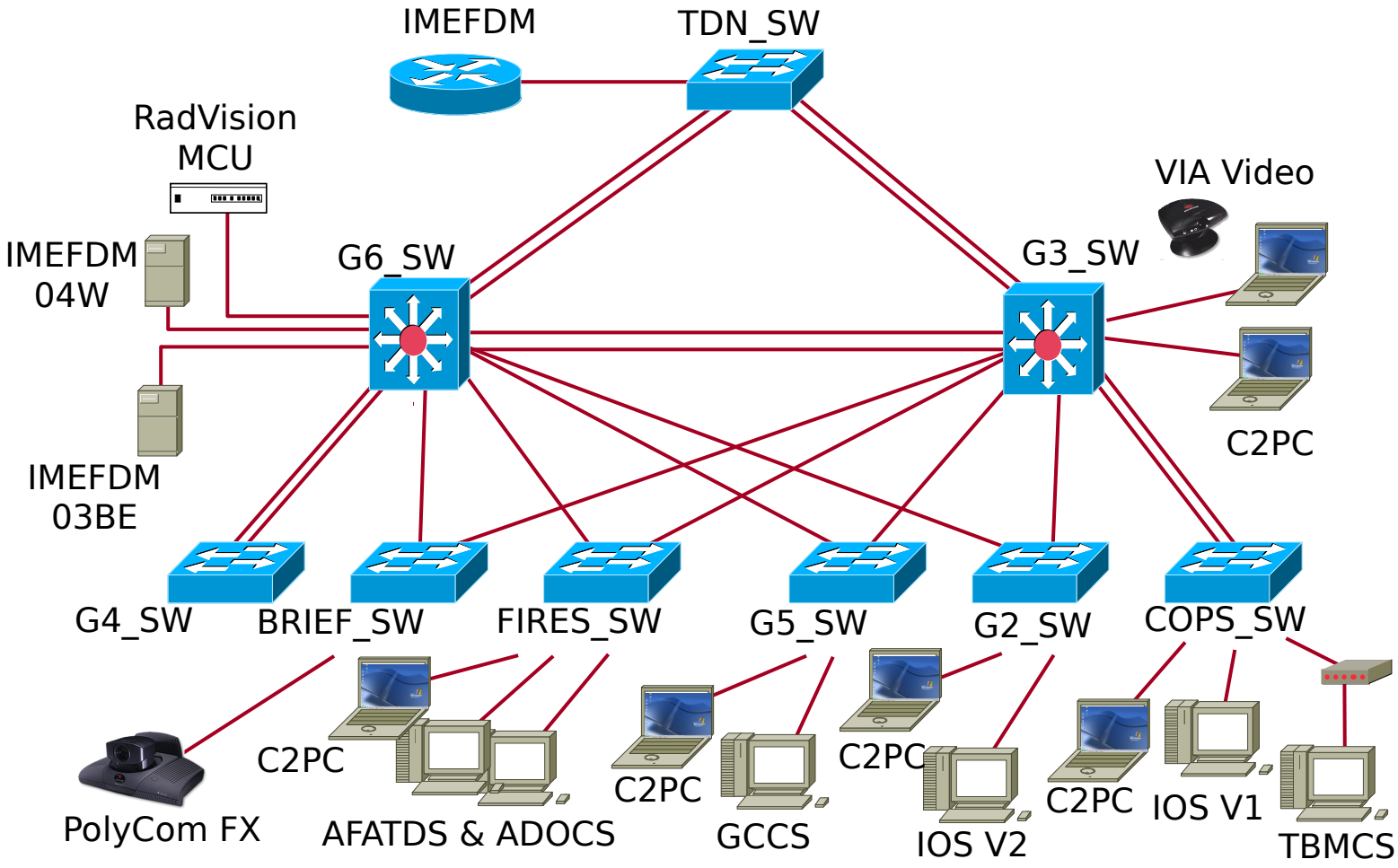


- Portfast BPDUGuard shuts down a switchport when a BPDU is received on that port.
- Port is down until manually reset.

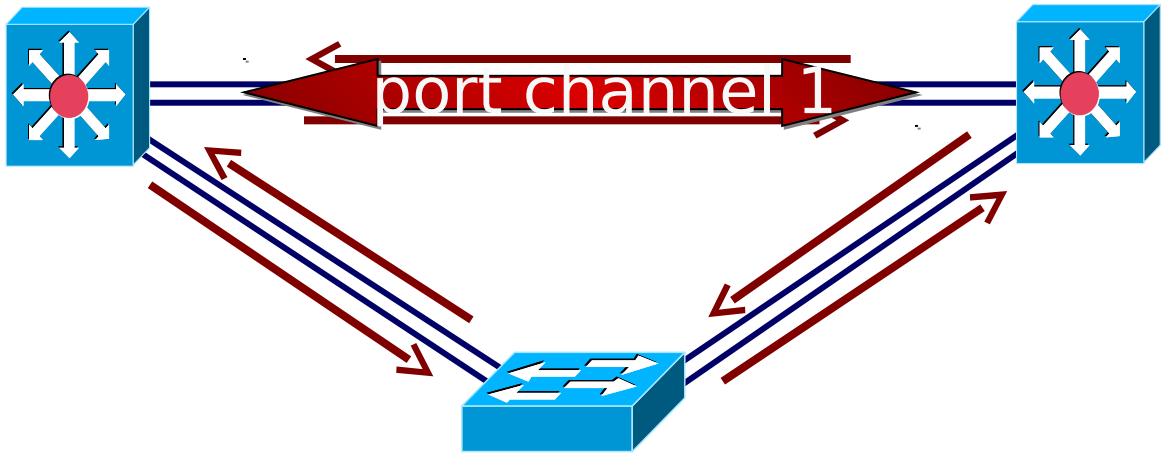
Advanced STP (cont.)

- Portfast BPDU filter
  - Prevents an interface from sending or receiving bridge protocol data units (BPDUs).
  - May be enabled per switch or per interface.
  - Effectively turns off STP on ports.

Switching Design (cont.)



EtherChannels



- An Etherchannel is simply a logical bundling of 2 - 8 physical connections between two Cisco switches.
- STP sees the Etherchannel as one connection. If any of the physical connections inside the Etherchannel go down, STP does not see this, and STP will not recalculate.

Planning Considerations

- Identify Port Assignments
- - Identify a policy of trunk port placement
- - Identify placement of root switch
- Plan for expansion
- - Never plan to use full port density on a switch

Step-by-Step (cont.)

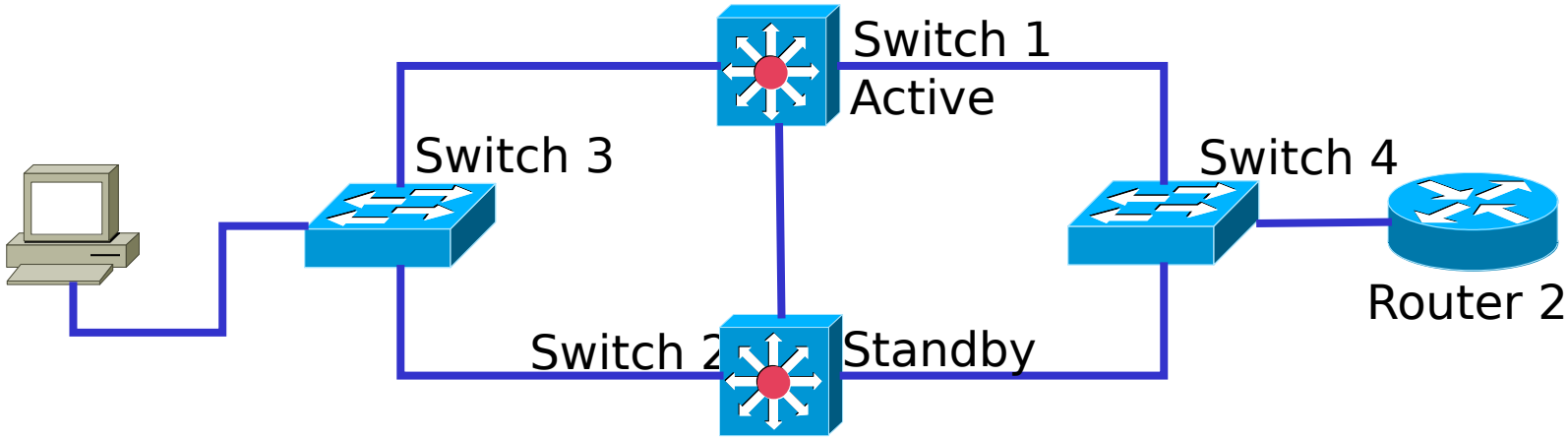

```
IMEF_S1(config)#span vlan 103 pri 16384
IMEF_S2(config)#span vlan 103 pri 20480
IMEF_S1(config)#span portf bpdug def
IMEF_S2(config)#int fa 1/0/12
IMEF_S2(config-if)#span portfast
IMEF_S2(config-if)#span bpdug enable
IMEF_S2(config-if)#span bpduf enable
IMEF_S2(config-if)#int ra fa 1/0/1 - 6
IMEF_S2(config-if)#channel-gr 1 mode on
IMEF_S2(config-if)#int port-channel 1
IMEF_S2(config-if)#end
IMEF_S2#
```

Lab #4

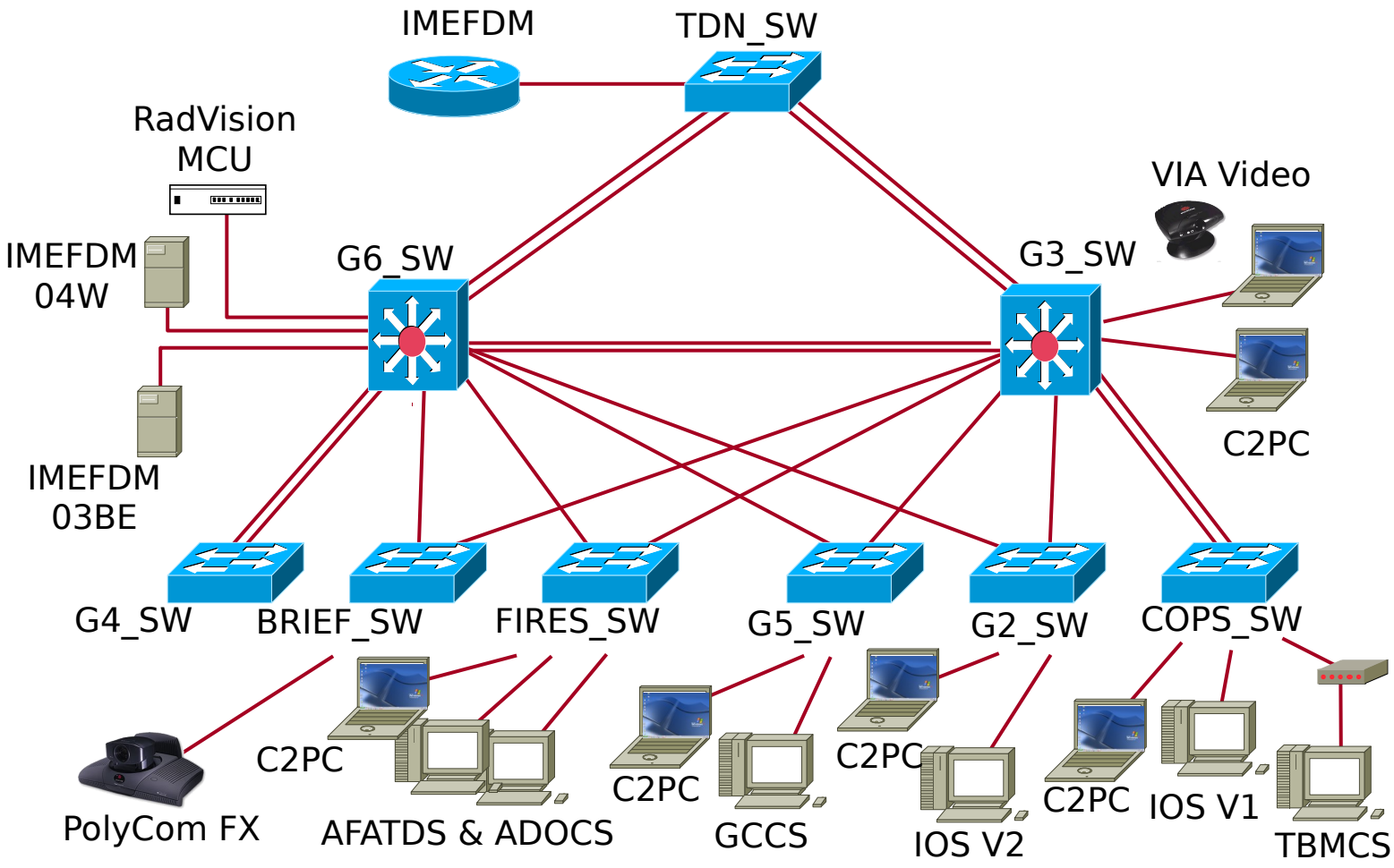
Configure Spanning-Tree, Control Root Bridge Selection & Configure Port Channels

Hot-Standby Routing Protocol

- Create virtual MAC address and IP
- Active Router acts as *virtual* Gateway
- Standby becomes active if Active Router Fails
- May be assigned per VLAN



Switching Design (cont.)



Inter-VLAN Routing

MSTP

```
IMEF_S1(config)#p routing
IMEF_S1(config)#int vlan 103
IMEF_S1(config-if)#ip address 200.54.111.67
255.255.255.240
IMEF_S1(config-if)#standby 103 ip
200.54.111.65
IMEF_S1(config-if)#stand 103 pri 200
IMEF_S1(config-if)#stand 103 preempt
```

Lab #5

Setup VLAN IP Addresses, IP Routing & HSRP

Questions